


NYPL RESEARCH LIBRARIES
3 3433 06909450 0



3-OGE

Web

Moker

LEHRBUCH

DER

ALGEBRA.

VON

HEINRICH WEBER,

PROFESSOR DER MATHEMATIK AN DER UNIVERSITÄT STRASSBURG.

IN ZWEI BÄNDEN.

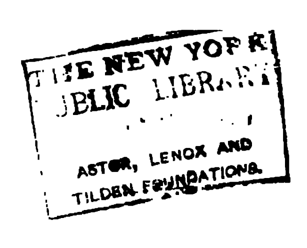
ZWEITER BAND.

BRAUNSCHWEIG,

DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN.

1896.

M.R.H.


THE NEW YORK
PUBLIC LIBRARY
ASTOR, LENOX AND
TILDEN FOUNDATIONS.

VORWORT ZUM ZWEITEN BANDE.

Der in dem Vorworte zum ersten Bande angekündigten Absicht gemäss kann ich heute den zweiten Band meines Lehrbuches der Algebra der Oeffentlichkeit übergeben. Der dort aufgestellte Plan ist in den wesentlichen Punkten durchgeführt. Bei den Anwendungen bin ich bemüht gewesen, solche Probleme auszuwählen, die bereits in anderen Gebieten, der Geometrie oder Functionentheorie, ein selbständiges Interesse gewonnen haben, und die zugleich die Hauptpunkte der algebraischen Theorie möglichst vielseitig zur Anschauung bringen.

Die Anwendung der Theorie der algebraischen Zahlen ist bis zur Theorie der Kreistheilungszahlen durchgeführt. Wenn Leben und Arbeitskraft vorhalten, hoffe ich, in einer Fortsetzung meines Werkes die weiteren Anwendungen auf das Gebiet der elliptischen Functionen darzustellen, die nur zum Theil in meinem Buche „Elliptische Functionen und algebraische Zahlen" enthalten sind.

Auch während der Ausarbeitung und des Druckes des zweiten Bandes hat mir die Hülfe und der Rath der Freunde zur Seite gestanden, die ich schon in der Vorrede zur ersten Auflage genannt habe. Aber auch manchen neuen Freund hat sich der erste Band bereits erworben, der meine Arbeit durch Winke und Rathschläge gefördert hat. Ihnen allen spreche ich an dieser Stelle meinen Dank aus, und füge die Bitte hinzu, dass sie dem Werke auch weiterhin ihr Interesse bewahren mögen.

Strassburg, im Juli 1896.

Der Verfasser.

INHALT DES ZWEITEN BANDES.

Erstes Buch.

Gruppen.

Erster Abschnitt.

Allgemeine Gruppentheorie.

Zweiter Abschnitt.

Abel'sche Gruppen.

Dritter Abschnitt.

Die Gruppe der Kreistheilungskörper.

Vierter Abschnitt.

Cubische und biquadratische Abel'sche Körper.

Fünfter Abschnitt.

Constitution der allgemeinen Gruppen.

Zweites Buch.

Lineare Gruppen.

Sechster Abschnitt.

Gruppen linearer Substitutionen.

Siebenter Abschnitt.

Gruppen binärer linearer Substitutionen.

Achter Abschnitt.

Die Polyëdergruppen.

Neunter Abschnitt.

Congruenzgruppen.

Drittes Buch.

Anwendungen der Gruppentheorie.

Zehnter Abschnitt.

Allgemeine Theorie der metacyklischen Gleichungen.

Elfter Abschnitt.

Die Wendepunkte einer Curve dritter Ordnung.

Zwölfter Abschnitt.

Die Doppeltangenten einer Curve vierter Ordnung.

Dreizehnter Abschnitt.

Allgemeine Theorie der Gleichung fünften Grades.

Vierzehnter Abschnitt.

Gruppen linearer ternärer Substitutionen.

Fünfzehnter Abschnitt.

Das Formenproblem der Gruppe G_{168} und die Theorie der Gleichungen siebenten Grades.

Viertes Buch.

Algebraische Zahlen.

Sechzehnter Abschnitt.

Zahlen und Functionale eines algebraischen Körpers.

Siebzehnter Abschnitt.

Theorie der algebraischen Körper.

Achtzehnter Abschnitt.

Discriminanten.

Neunzehnter Abschnitt.

Beziehung eines Körpers auf seine Theiler.

Zwanzigster Abschnitt.

Quadratische Körper.

Einundzwanzigster Abschnitt.

Kreistheilungskörper.

Zweiundzwanzigster Abschnitt.

Abel'sche Körper und Kreistheilungskörper.

Dreiundzwanzigster Abschnitt.

Classenzahl.

Vierundzwanzigster Abschnitt.

Classenzahl der Kreistheilungskörper.

Fünfundzwanzigster Abschnitt.

Transcendente Zahlen.

Nachträge.

ERSTES BUCH.

GRUPPEN.

Erster Abschnitt.

Allgemeine Gruppentheorie.

---

§. 1.
Definition der Gruppen.

Wir haben im ersten Bande bei den Permutationen den Begriff einer Gruppe kennen gelernt und wichtige algebraische Anwendungen von ihm gemacht. Es muss nun unsere nächste Aufgabe sein, diesen in der ganzen neueren Mathematik so überaus wichtigen Begriff allgemeiner zu fassen und die dabei herrschenden Gesetze kennen zu lernen. Wir stellen folgende Definition an die Spitze:

Ein System P von Dingen (Elementen) irgend welcher Art wird zur Gruppe, wenn folgende Voraussetzungen erfüllt sind:

1. Es ist eine Vorschrift gegeben, nach der aus einem ersten und einem zweiten Elemente des Systems ein ganz bestimmtes drittes Element desselben Systems abgeleitet wird.

Man schreibt symbolisch, wenn a das erste, b das zweite, c das dritte Element ist:

$$ab = c, \quad c = ab,$$

und nennt c aus a und b componirt und a und b die Componenten von c.

Bei dieser Composition wird im Allgemeinen nicht das commutative Gesetz vorausgesetzt, d. h. es kann ab von ba verschieden sein, dagegen wird

2. das associative Gesetz vorausgesetzt,

d. h. wenn a, b, c irgend drei Elemente aus P sind, so ist

$$(ab)c = a(bc),$$

und hieraus folgt durch die Schlussweise der vollständigen Induction, dass man immer zu demselben Resultate kommt, wenn man in einer beliebigen Reihe von Elementen aus P in endlicher Anzahl, $a, b, c, d \ldots$ zuerst zwei benachbarte Elemente componirt, dann wieder zwei benachbarte u. s. w., bis die ganze Reihe auf ein Element reducirt ist, das mit $a\,b\,c\,d \ldots$ bezeichnet wird. So ist z. B.:

$$\begin{aligned} abcd &= (ab)cd = [(ab)c]d = (ab)(cd) \\ &= a(bc)d = [a(bc)]d = a[(bc)d] \\ &= ab(cd) = (ab)(cd) = a[b(cd)] \end{aligned}$$ [1].

3. Es wird vorausgesetzt, dass, wenn $ab = ab'$ oder $ab = a'b$ ist, nothwendig im ersten Falle $b = b'$, im zweiten $a = a'$ sein muss.

Wenn P eine endliche Anzahl von Elementen umfasst, so heisst die Gruppe eine endliche und die Anzahl ihrer Elemente ihr Grad.

Für endliche Gruppen ergiebt sich aus 1., 2., 3. die Folgerung:

4. Wenn von den drei Elementen a, b, c aus P zwei beliebig gegeben sind, so kann man das dritte immer und nur auf eine Weise so bestimmen, dass

$$ab = c$$

ist.

Sind nämlich a, b die gegebenen Elemente, so fällt die Behauptung 4. mit 1. zusammen. Ist aber a und c gegeben, so lasse man in dem Compositum ab die zweite Componente b das ganze System P durchlaufen, dessen Grad $= n$ sei. Dann erhält man nach 1. und 3. in ab lauter verschiedene Elemente von P, und da ihre Anzahl $= n$ ist, so müssen alle Elemente von P, also auch c, darunter vorkommen. Ebenso schliesst man, wenn b und c gegeben sind, indem man a das ganze System P durchlaufen lässt.

Für unendliche Gruppen kann nicht mehr so geschlossen werden. Für unendliche Gruppen wird also noch die Eigenschaft 4. als Forderung in die Begriffsbestimmung mit aufgenommen.

---

[1] Vgl. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, §. 2.

Bei den im ersten Bande betrachteten Permutationsgruppen wird man leicht die Merkmale des allgemeinen Gruppenbegriffes erkennen.

Wir ziehen nun aus dieser Definition zunächst einige ganz allgemeine Folgerungen.

Nach 4. giebt es für jedes gegebene b **ein** Element e in P, das der Bedingung

(1) $$eb = b$$

genügt, und dies e ist von b unabhängig; denn aus (1) folgt für jedes c

$$ebc = bc,$$

und bc kann nach 4. jedes Element in P bedeuten. Ebenso giebt es ein Element e', das für jedes b der Bedingung

(2) $$be' = b$$

genügt. Dies Element e' ist aber von e nicht verschieden; denn setzen wir $b = e'$ in (1) und $b = e$ in (2), so folgt

$$ee' = e', \quad ee' = e,$$

also

$$e = e'.$$

Das Element e ändert nichts, wenn es mit irgend welchen Elementen aus P componirt wird, und wird die **Einheit der Gruppe** genannt.

In vielen Fällen kann es ohne Missverständniss geradezu mit „1" bezeichnet werden.

Zu jedem Element a giebt es nach 4. ein bestimmtes Element a^{-1}, das der Bedingung

(3) $$a^{-1}a = e$$

genügt. Aus (3), (1) und (2) folgt

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1} = a^{-1}e,$$

und folglich nach 3.

(4) $$aa^{-1} = e.$$

Die beiden Elemente a, a^{-1} heissen zu einander **entgegengesetzt** oder **reciprok**.

In besonderen Fällen kann bei der Composition der Elemente einer Gruppe P auch das commutative Gesetz gelten, d. h. es kann für je zwei Elemente a, b der Gruppe

$$ab = ba$$

sein.

Elfter Abschnitt.

Die Wendepunkte einer Curve dritter Ord.

Zwölfter Abschnitt.

Die Doppeltangenten einer Curve vierter Ord.

Dreizehnter Abschnitt.

Allgemeine Theorie der Gleichung

Seite

…per.

Viertes Buch.

Q_1 verschieden sind. Denn wäre etwa $a_1 c = a_2 b$, so würde folgen, dass $c = a_1^{-1} a_2 b$ sein müsste; es ist aber $a_1^{-1} a_2$ in Q enthalten, also mit einem der Elemente $1, a_1, a_2 \dots a_{\nu-1}$ identisch, und es wäre also c gegen die Voraussetzung in Q_1 enthalten. So fahren wir fort, die Systeme $Q, Q_1, Q_2 \dots Q_{\mu-1}$ zu bilden, von denen das letzte

$$Q_{\mu-1} = g, a_1 g, a_2 g \dots a_{\nu-1} g$$

sei. Dann muss aber P durch die Systeme $Q, Q_1, Q_2 \dots Q_{\mu-1}$ erschöpft sein, und es folgt, da diese Systeme lauter verschiedene Elemente enthalten,

$$n = \nu \mu,$$

oder der Satz:

1. Der Grad einer Gruppe ist durch den Grad jedes ihrer Divisoren theilbar. Der Quotient $\mu = n : \nu$ soll der Index des Theilers Q heissen.

Die Systeme $Q_1, Q_2 \dots Q_{\mu-1}$ nennen wir, wie in dem speciellen Falle der Permutationsgruppen, die zu Q gehörigen Nebengruppen und bezeichnen sie durch

$$Q_1 = Qb, \quad Q_2 = Qc \dots \quad Q_{\mu-1} = Qg,$$

so dass wir auch symbolisch

$$(1) \qquad P = Q + Qb + Qc + \cdots + Qg$$

setzen können.

Bisweilen werden wir auch das ganze System $Q, Q_1 \dots Q_{\mu-1}$ (Q selbst eingeschlossen) als ein System von Nebengruppen bezeichnen, und also die Darstellung (1) die Zerlegung von P in ein System von Nebengruppen nennen.

Aus der Bildungsweise der Nebengruppen folgt noch, dass, wenn b, c irgend zwei Elemente aus P sind, die beiden Systeme Qb und Qc entweder ganz identisch sind oder kein gemeinsames Element enthalten. Denn ist $a_1 b = a_2 c$, worin a_1, a_2 zwei Elemente aus Q sind, so ist auch für jedes andere Element a aus Q:

$$a a_1 b = a a_2 c,$$

und wenn a die ganze Gruppe Q durchläuft, so durchläuft, wie schon in §. 1 bemerkt, auch jedes der beiden $a a_1$ und $a a_2$ die ganze Gruppe Q; folglich sind Qb und Qc identisch.

Wie in Bd. I, §. 154, 2. können wir P auch in der folgenden Art in Nebengruppen zerlegen:

$$P = Q + b^{-1} Q + c^{-1} Q + \cdots + g^{-1} Q.$$

Die Nebengruppen haben nicht die Merkmale einer Gruppe. Denn damit zwei Elemente aus Q_1 bei der Zusammensetzung wieder ein Element von Q_1 ergeben, müsste etwa

$$a_1 b a_2 b = a_3 b,$$

also $a_1 b a_2 = a_3$, $b = a_1^{-1} a_3 a_2^{-1}$ sein. Es wäre also b der Voraussetzung entgegen in Q enthalten.

Die Benennung Nebengruppe ist also nur uneigentlich zu verstehen.

Zwei Theiler Q, Q' von P haben immer das Element 1 mit einander gemein. Sie können aber auch noch andere Elemente gemeinschaftlich haben, und diese gemeinschaftlichen Elemente bilden eine Gruppe, die wir mit R bezeichnen wollen. Denn gehören die Elemente a und b sowohl zu Q als zu Q', so gilt wegen des Gruppencharakters von Q und Q' dasselbe von dem Compositum ab; also ist R eine Gruppe. Diese gemeinschaftliche Gruppe nennen wir den grössten gemeinschaftlichen Theiler von Q und Q' oder auch, mit einem geometrischen Anklange, den Durchschnitt von Q und Q'. Ebenso folgt, dass die Elemente, die irgend einer Anzahl von Theilern von P gemeinsam sind, eine Gruppe bilden, die wir ebenso als den grössten gemeinschaftlichen Theiler oder den Durchschnitt aller dieser Gruppen bezeichnen.

In jeder Gruppe können wir nach folgendem Verfahren Theiler bilden.

Ein Theiler ist immer das Einheitselement für sich.

Bezeichnen wir die wiederholte Zusammensetzung eines Elementes mit sich selbst durch Potenzen (mit a^0 das Einheitselement), so kann die Reihe der Elemente

$$1, a, a^2, a^3 \ldots,$$

die alle der Gruppe P angehören, nicht lauter verschiedene Elemente enthalten. Ist also das erste Element, das zum zweiten Male wiederkehrt,

$$a^\mu = a^{\mu + \alpha},$$

so folgt, dass $a^\alpha = 1$ sein muss, und dass α die kleinste positive Zahl ist, die dieser Bedingung genügt. Es ist dann, wenn $m = q\alpha$ ein beliebiges Vielfaches von α ist, $a^m = 1$ und umgekehrt: so oft $a^m = 1$ ist, muss m durch α theilbar sein; denn sonst könnte man $m = q\alpha + \alpha'$ setzen, worin α' positiv und kleiner als α ist, und es wäre $a^{\alpha'} = 1$, gegen die Voraussetzung,

dass α der kleinste positive Exponent sei, für den $a^\alpha = 1$ ist. Es ist immer und nur dann

$$a^\mu = a^{\mu'},$$

wenn $\mu \equiv \mu'$ (mod α), und hierin können die Exponenten auch negativ sein, wenn a^{-r} die r^{te} Potenz des Elementes a^{-1} oder das zu a^r entgegengesetzte Element bedeutet.

Die Reihe

$$A = 1,\ a,\ a^2 \ldots a^{\alpha-1}$$

enthält dann α von einander verschiedene Elemente von P, wobei alle Potenzen von a vertreten sind. Die Elemente A bilden aber offenbar eine Gruppe vom Grade α, weil sich die Exponenten bei der Zusammensetzung einfach addiren. Diese Gruppe ist ein Theiler von P und also ist α ein Theiler von n. Es ist also für jedes Element $a^n = 1$.

Die Gruppe A heisst die Periode des Elementes a und α wird auch der Grad des Elementes a genannt.

§. 3.

Normaltheiler einer Gruppe.

Ist P wie oben eine Gruppe und Q ein Divisor von P, ferner b ein nicht in Q enthaltenes Element von P, so ist die Nebengruppe $Q\,b$ keine Gruppe. Dagegen bildet das System $b^{-1}\,Q\,b$, oder ausführlich geschrieben

$$1,\ b^{-1}a_1 b,\ \ b^{-1}a_2 b \ldots\ \ b^{-1}a_{\nu-1} b$$

sicher eine Gruppe, weil

$$b^{-1}a_1 b\ .\ b^{-1}a_2 b = b^{-1}a_1 a_2 b$$

ist, und diese Gruppe ist mit Q isomorph. Die Gruppe $b^{-1}\,Q\,b$ heisst die durch b transformirte Gruppe. Gehört b selbst zu Q, so ist $b^{-1}\,Q\,b$ mit Q identisch. Nimmt man für b die verschiedenen Elemente von P, so erhält man eine ganze Schaar solcher Gruppen, die wir die zu Q conjugirten Theiler von P oder auch kurz conjugirte Gruppen nennen.

Es kann vorkommen, dass alle conjugirten Theiler mit einander identisch sind. Wir haben schon bei den Permutationsgruppen gesehen, dass dieser Fall von besonderer Wichtigkeit ist, und führen also nun allgemein folgende Definition ein:

Wenn Q ein Theiler von P ist, der mit seinen sämmtlichen conjugirten Theilern identisch ist, so heisst Q ein Normaltheiler von P[1]).

Die aus dem einzigen Element 1 gebildete Gruppe ist ein Normaltheiler von jeder Gruppe. Wir erhalten ferner einen Normaltheiler in dem grössten gemeinschaftlichen Theiler R der sämmtlichen mit irgend einem Theiler Q von P conjugirten Theiler.

Denn es ist schon oben bewiesen, dass R als der Durchschnitt mehrerer Theiler von P eine Gruppe ist.

Sind nun

(1) $$Q,\ Q',\ Q'' \ldots$$

die zu Q conjugirten Theiler von P und b irgend ein Element von P, dann ist das System der Gruppen

(2) $$b^{-1}Qb,\quad b^{-1}Q'b,\quad b^{-1}Q''b \ldots$$

von dem System (1) nicht verschieden. Wenn aber R der Durchschnitt der Gruppen (1) ist, so ist $b^{-1}Rb$ der Durchschnitt von (2), und folglich ist R mit $b^{-1}Rb$ identisch, d. h. R ist ein Normaltheiler von P.

Ist N ein Normaltheiler irgend einer Gruppe P und b ein beliebiges Element in P; so ist

(3) $$b^{-1}Nb = N \quad \text{oder} \quad Nb = bN.$$

Ist P vom Grade n, N vom Grade ν und vom Index μ, also $n = \mu\nu$, so können wir die μ Elemente $1, b_1 \ldots b_{\mu-1}$ so wählen, dass die Zerlegung von P in die Nebengruppen

$$\begin{aligned} P &= N + Nb_1 + Nb_2 + \cdots + Nb_{\mu-1} \\ &= N + b_1N + b_2N + \cdots + b_{\mu-1}N \end{aligned}$$

ergiebt. Es ist also

(4) $$N,\ N_1 = Nb_1 = b_1N,\ N_2 = Nb_2 = b_2N \ldots,\quad N_{\mu-1} = Nb_{\mu-1} = b_{\mu-1}N$$

das System der Nebengruppen.

Ist a irgend ein Element in N, so ist Na mit N identisch, also ist auch Nab mit Nb identisch, und da jedes Element c von P in N oder in einer seiner Nebengruppen vorkommt, also in der Form ab_k enthalten ist, so muss $Nc = cN$ mit einem der Systeme (4) übereinstimmen.

---

[1]) Auch ausgezeichnete oder invariante Untergruppe genannt.

Wir erwähnen noch folgenden Satz, dessen Richtigkeit sich unmittelbar aus dem Isomorphismus transformirter Gruppen ergiebt:

Ist Q ein Theiler von P, R ein Theiler von Q, so ist, wenn Q' und R' aus Q und R durch dasselbe Element von P transformirt sind, auch R' ein Theiler von Q', und wenn R Normaltheiler von Q ist, so ist auch R' Normaltheiler von Q'.

§. 4.

Composition der Theile.

Sind A und B irgend zwei Reihen von Elementen aus einer Gruppe P (Gruppen oder nicht), so wollen wir unter dem symbolischen Producte AB den Inbegriff aller Elemente verstehen, die man erhält, wenn man je ein Element a von A mit je einem Element b von B nach der in P geltenden Vorschrift zu ab componirt. Diese Art der Zusammensetzung von A und B zu AB wollen wir die Composition der Theile (von P) nennen. Wir unterscheiden hier zwischen einem Theil und einem Theiler von P, so dass ein Theiler immer eine Gruppe sein soll, was bei einem Theil nicht nothwendig ist.

Man kann ebenso drei und mehr Theile $A, B, C \dots$ von P componiren, und es gilt bei der Composition der Theile das associative Gesetz, wie unmittelbar daraus folgt, dass dieses Gesetz in P gilt. Danach ist die Bedeutung eines Compositums $ABC \dots$ eindeutig bestimmt.

In der Zusammensetzung AB kann einer der Theile A, B auch aus einem einzigen Elemente bestehen, und dann stimmt die Bezeichnung AB mit der oben für die Nebengruppen gebrauchten Bezeichnung überein.

Bei der Composition der Theile gelten folgende Sätze:

1. Die nothwendige und hinreichende Bedingung dafür, dass ein Theil A von P eine Gruppe ist, besteht in der Gleichung

(1) $$AA = A.$$

Denn diese Gleichung besagt nichts Anderes als dass, wenn a und a' in A enthalten sind, auch aa' zu A gehört, also dass A eine Gruppe ist.

2. Durch die beiden Gleichungen

$$AA = A, \tag{2}$$

$$AB = BA, \tag{3}$$

worin A ein bestimmter, B jeder beliebige Theil von P sein kann, wird ausgesagt, dass A ein Normaltheiler von P ist.

Denn nach (2) ist A ein Theiler von P und nach (3) ist für jedes Element b von P

$$b^{-1}Ab = A,$$

d. h. A ist ein Normaltheiler.

3. Sind A und B zwei Theiler von P (Gruppen), so ist eine der beiden Gleichungen

$$AB = A, \quad BA = A, \tag{4}$$

die nothwendige und hinreichende Bedingung dafür, dass B ein Theiler von A ist.

Denn wenn B eine Gruppe und ein Theiler der Gruppe A ist, und wenn a in A, b in B und also auch in A enthalten ist, so ist auch ab in A enthalten. A enthält also jedes Element von AB.

Weil aber zweitens B als Gruppe auch das Element 1 enthält, so enthält AB auch jedes Element von A, und also ist AB mit A identisch.

Ebenso sieht man, dass BA mit A identisch ist. Andererseits folgt aus jeder der Gleichungen (4), da A als Gruppe das Einheitselement enthält, dass jedes Element von B in A enthalten, also B ein Theiler von A ist.

4. Bei der Composition der Theile bildet das System der Nebengruppen zu einem Normaltheiler von P selbst eine Gruppe, in der der Normaltheiler N die Einheit bildet, und

$$Nb, \quad Nb^{-1}$$

entgegengesetzte Elemente sind.

Denn ist N ein Normaltheiler von P und

$$N, \; N_1 = Nb_1, \; N_2 = Nb_2, \ldots \tag{5}$$

das System der Nebengruppen, so ist

$$N_h N_k = Nb_h Nb_k.$$

Wegen der Eigenschaft der Normaltheiler ist aber N mit jedem b vertauschbar, also $b_h N = N b_h$, und folglich

$$N_h N_k = N N b_h b_k.$$

Weil $b_h b_k$ in P enthalten ist, so ist $N b_h b_k$ mit einer der Nebengruppen (5) identisch, und da $NN = N$ gesetzt werden kann (nach 1.), so folgt, wenn wir $N b_h b_k = N_l$ setzen,

(6) $$N_h N_k = N_l.$$

Damit ist die Eigenschaft §. 1, 1. der Gruppen für die Composition der Nebengruppen nachgewiesen. Dass auch §. 1, 2., nämlich das associative Gesetz gilt, haben wir schon hervorgehoben. Es ist also noch §. 1, 3. nachzuweisen, nämlich dass, wenn

(7) $$N_h N_i = N_k N_l$$

gesetzt wird, und $N_h = N_k$ ist, auch $N_i = N_l$, und wenn $N_i = N_l$ ist, auch $N_h = N_k$ sein muss.

Nach der Darstellung (5) können wir aber (7) in der doppelten Weise darstellen:

(8) $$\begin{aligned} N b_h b_i &= N b_k b_l \\ b_h b_i N &= b_k b_l N. \end{aligned}$$

Ist nun $N_i = N_l$, so können wir auch $b_i = b_l$ annehmen, und erhalten aus (8) durch Composition mit b_i^{-1}

$$N b_h = N b_k;$$

und wenn $N b_h = N b_k$ ist, so nehmen wir $b_h = b_k$ an und erhalten aus (8) durch Composition mit b_h^{-1}

$$b_i N = b_l N,$$

also auch $N_i = N_l$.

Damit ist also erwiesen, dass das System der Nebengruppen durch die Composition der Theile zu einer Gruppe wird; dass in dieser Gruppe der Normaltheiler N das Einheitselement ist, folgt unmittelbar aus 1., weil danach

$$N N_k = N N b_k = N_k$$

ist. Und weil $N b_k N b_k^{-1} = N b_k b_k^{-1} = N$ ist, so sind $N b_k$ und $N b_k^{-1}$ entgegengesetzte Elemente.

Die Gruppe der Grössen N_k, deren Existenz also hiermit nachgewiesen ist, nennen wir die Gruppe der Nebengruppen oder die zu N complementäre Gruppe in Bezug auf P. Wir

bezeichnen sie nach dem Vorgange von Hölder[1]) mit P/N. Der Grad der complementären Gruppe ist gleich dem Index der Gruppe N.

Wir erwähnen am Schluss dieser Betrachtungen noch einen Satz über Normaltheiler.

5. Ist N ein Theiler von P, N' ein Theiler von N und zugleich Normaltheiler von P, so ist auch N' Normaltheiler von N.

Dies ist selbstverständlich, weil für jedes Element b von P $b^{-1}N'b = N'$ ist, und weil jedes Element von N auch ein Element von P ist.

Man darf aber nicht umgekehrt schliessen, dass, wenn N ein Normaltheiler von P, N' ein Normaltheiler von N ist, auch N' ein Normaltheiler von P sein müsse.

§. 5.

Mehrstufiger Isomorphismus.

Ist wie oben N ein Normaltheiler von P vom Grade ν und Index μ, also $n = \mu\nu$, so ist die zu P complementäre Gruppe P/N vom Grade μ. Wir wollen diese oder eine damit isomorphe Gruppe mit Q bezeichnen und ihre Elemente, die den Nebengruppen N, Nb_1, Nb_2 ... entsprechen, mit A, B, C ... Jedem dieser Elemente entsprechen ν Elemente der Gruppe P, etwa

dem Elemente A die Elemente $a, a_1 \ldots a_{\nu-1}$
dem Elemente B die Elemente $b, b_1 \ldots b_{\nu-1}$
. . . .

Dies Entsprechen ist dann derart, dass jedes zusammengesetzte Element ab dem zusammengesetzten Elemente AB entspricht. Denn die Elemente A und B entsprechen den Nebengruppen Na und Nb, und es ist, weil N ein Normaltheiler ist,

$$Na\,Nb = Nab.$$

Es gilt also hier bei der Zusammensetzung der A, B ... einerseits und der a, b ... andererseits dasselbe Gesetz, wie bei

[1]) Mathematische Annalen, Bd. 34. Das Zeichen erinnert an einen Quotienten, mit dem ja die complementäre Gruppe eine gewisse Analogie hat.

den isomorphen Gruppen (§. 1), nur mit dem Unterschiede, dass jedem Elemente A nicht bloss ein Element a, sondern mehrere entsprechen. Diese Thatsache giebt Anlass, den Begriff des Isomorphismus zu erweitern, wie es durch folgende Definition geschieht:

Man nennt eine Gruppe P mit den Elementen $a, b, c \dots$ (mehrstufig) isomorph mit einer Gruppe Q mit den Elementen $A, B, C \dots$, wenn beide Gruppen so auf einander bezogen werden können, dass jedem der Elemente $A, B, C \dots$ ein oder mehrere der Elemente $a, b, c \dots$ entsprechen, und zwar so, dass jedes der Elemente von Q einem und nur einem der Elemente von P entspricht, und dass, wenn a und A, b und B einander entsprechen, ab dem Elemente AB entspricht.

So lässt sich zunächst beweisen, dass jedem der Elemente $A, B, C \dots$ eine gleiche Zahl von Elementen $a, b, c \dots$ entspricht und dass also der Grad von Q ein Theiler des Grades von P ist. Denn es sei A das Einheitselement in Q, dem die Elemente $a, a_1 \dots a_{\nu-1}$ in P entsprechen mögen. Diese letzteren Elemente müssen dann eine Gruppe vom Grade ν bilden, die wir mit N bezeichnen wollen, weil nach der Definition des Isomorphismus das Element $a a_1$ dem Elemente $AA = A$ entsprechen muss. Ist dann b ein dem Elemente B entsprechendes Element von P, so müssen wiederum alle Elemente Nb demselben Elemente B aus Q entsprechen. Denn jedes ab muss dem Elemente $AB = B$ entsprechen. Sind b_1, b zwei dem Elemente B entsprechende Elemente, so entspricht $b_1 b^{-1} = a$ dem Elemente A, und ist also in N enthalten, also ist $b_1 = ab$ in Nb enthalten. Durch Nb sind also alle Elemente, die dem Elemente B entsprechen, erschöpft, und jedem Elemente von Q entsprechen ν Elemente von P. Der Isomorphismus heisst ν-stufig. Jedes Element $b^{-1}ab$ entspricht aber gleichfalls dem Einheitselemente A und also ist $b^{-1}Nb = N$, d. h. N ist Normaltheiler von P, und Q ist einstufig isomorph mit P/N.

Wir sehen also, dass es einen anderen mehrstufigen Isomorphismus als den zwischen der complementären Gruppe eines Normaltheilers und der Gesammtgruppe nicht giebt. Man könnte aber den Begriff des Isomorphismus noch dahin erweitern, dass man zwei Gruppen, die zu einer dritten Gruppe μ- und ν-stufig

isomorph sind, μ-ν-stufig isomorph zu einander nennt. Bei Weitem der wichtigste ist der einstufige Isomorphismus, den wir daher als Isomorphismus schlechtweg bezeichnen, während ein mehrstufiger Isomorphismus immer durch einen Zusatz kenntlich gemacht werden soll [1]).

§. 6.

Die Compositionsreihe und der Satz von C. Jordan.

Eine Gruppe P heisst einfach, wenn sie ausser sich selbst und der Einheit keinen Normaltheiler hat, zusammengesetzt, wenn noch andere Normaltheiler vorhanden sind.

Ein Normaltheiler, der keinen anderen Normaltheiler über sich hat, der also nicht Theil eines anderen echten Normaltheilers von P ist, heisst ein grösster Normaltheiler von P [2]). Ist P_1 ein grösster Normaltheiler von P, P_2 ein grösster Normaltheiler von P_1, P_3 ein grösster Normaltheiler von P_2 u. s. f., so heisst die Reihe von Gruppen

(1) $$P,\ P_1,\ P_2,\ P_3 \ldots 1,$$

die nothwendig mit der aus dem Einheitselemente allein gebildeten Gruppe 1 endigt, eine Compositionsreihe der Gruppe P.

Wir wollen die Grade der Gruppen (1) mit $n, n_1, n_2, n_3 \ldots 1$ bezeichnen, und die Quotienten $n : n_1$, $n_1 : n_2$, $n_2 : n_3 \ldots$, also die Indices von P_1 in Bezug auf P, P_2 in Bezug auf P_1 u. s. f. mit $\nu_1, \nu_2, \nu_3 \ldots$ Die Reihe der ganzen Zahlen

(2) $$\nu_1,\ \nu_2,\ \nu_3 \ldots$$

nennen wir die Indexreihe der Gruppe P.

Die grössten Normaltheiler $P_1, P_2, P_3 \ldots$ können für eine gegebene Gruppe P im Allgemeinen auf mehrere verschiedene Arten ausgewählt werden, und danach können auch die Gradzahlen $n_1, n_2, n_3 \ldots$ und die Indices $\nu_1, \nu_2, \nu_3 \ldots$ verschieden

---

[1]) Vgl. C. Jordan, Traité des substitutions. Netto, Substitutionentheorie. Die Bezeichnung „μ-stufig" rührt von Netto her. Nach Jordan heisst der einstufige Isomorphismus „holoëdrischer", der mehrstufige „meroëdrischer" Isomorphismus. Der einstufige Isomorphismus wird bisweilen auch als Aequivalenz bezeichnet.

[2]) Ausgezeichnete Maximal-Untergruppe nach anderer Bezeichnung.

ausfallen. Es gilt aber der folgende schöne und wichtige Satz von C. Jordan [1]):

I. **Wie auch die Compositionsreihe einer Gruppe P gewählt sein mag, die Indexreihe ist, von der Anordnung abgesehen, immer dieselbe.**

Der Beweis beruht auf der Betrachtung der im vorigen Paragraphen eingeführten complementären Gruppen.

Es seien Q und Q_1 Normaltheiler von P und zugleich Q_1 ein Theiler (also nach §. 4, 5. Normaltheiler) von Q.

Dann gilt der Satz:

1. **Die Gruppe Q/Q_1 ist ein Normaltheiler der Gruppe P/Q_1, und der Index von Q/Q_1 in Bezug auf P/Q_1 ist gleich dem Index von Q in Bezug auf P.**

Um seine Richtigkeit einzusehen, braucht man nur die Bildungsweise der einzelnen Gruppen genauer zu betrachten.

Es seien n, q, q_1 die Grade von P, Q, Q_1 und

$$n = \nu q, \quad q = \nu_1 q_1, \quad n = \mu q_1, \quad \mu = \nu \nu_1. \tag{3}$$

Man zerlegt nun Q in die Nebengruppen zu Q_1, d. h. man setzt, wenn $b_1, b_2 \ldots b_{\nu_1 - 1}$ passend bestimmte Elemente in Q sind,

$$Q = Q_1 + Q_1 b_1 + \cdots Q_1 b_{\nu_1 - 1}. \tag{4}$$

Die Elemente der Gruppe Q/Q_1 sind

$$Q_1, Q_1 b_1, \ldots Q_1 b_{\nu_1 - 1}. \tag{5}$$

Wenn wir P in die Nebengruppen zu Q_1 zerlegen, so kommen darunter sicher die Elemente (5) vor, und folglich ist Q/Q_1 ein Theiler von P/Q_1.

Es ist also noch nachzuweisen, dass dieser Theiler ein Normaltheiler ist.

Bezeichnen wir aber mit a irgend ein Element von P, so sind alle Elemente von P/Q_1 in der Form $Q_1 a$ enthalten, und wir haben also nur zu zeigen, dass, wenn b irgend ein Element in Q ist, jedes Element

$$Q_1 a^{-1} Q_1 b Q_1 a \tag{6}$$

in Q/Q_1, d. h. in der Form $Q_1 b$ enthalten ist.

---

[1]) C. Jordan, Traité des substitutions, Paris 1870. Netto, Substitutionentheorie, Leipzig 1882. Wir folgen hier dem Beweise, den Hölder im Anschluss an Netto gegeben hat (Math. Annalen, Bd. 34).

Dies folgt aber unmittelbar aus

(7) $$Q_1 a^{-1} Q_1 b Q_1 a = Q_1 a^{-1} b a,$$

weil zugleich mit b auch $a^{-1} b a$ in Q vorkommt (weil Q ein Normaltheiler von P ist). Und dass auch die Bestimmung der Indices richtig ist, zeigt die Abzählung. Denn die Grade von P/Q_1 und Q/Q_1 sind $\nu \nu_1$ und ν_1, also der Index ν.

Daneben besteht folgender Satz:

2. Ist Q_1 ein Normaltheiler von P vom Grade q_1, und hat die Gruppe P/Q_1 selbst einen Theiler M vom Grade m, so hat P einen Theiler Q vom Grade $q = m q_1$. Zugleich ist Q_1 ein Normaltheiler von Q, und es ist $M = Q/Q_1$. Ist M Normaltheiler von P/Q_1, so ist auch Q Normaltheiler von P.

Es sei μ der Index von Q_1 in Bezug auf P, und P sei in die Nebengruppen zerlegt:

(8) $$P = Q_1 + Q_1 e_1 + Q_1 e_2 \cdots + Q_1 e_{\mu-1},$$

so dass $e_1, e_2 \ldots e_{\mu-1}$ passend gewählte Elemente in P und

(9) $$Q_1,\ Q_1 e_1,\ Q_1 e_2 \ldots Q_1 e_{\mu-1}$$

die Elemente von P/Q_1 sind. Wenn nun in der Gruppe P/Q_1 ein Theiler M enthalten ist, so muss dieser aus einem Theile der Elemente (9) bestehen, etwa aus

(10) $$Q_1,\ Q_1 b_1,\ Q_1 b_2 \ldots Q_1 b_{\nu_1-1},$$

und wenn dies System eine Gruppe bilden soll, so muss für irgend zwei Elemente b_i, b_k das Product

(11) $$Q_1 b_i Q_1 b_k = Q_1 b_i b_k$$

wieder in (10) enthalten, also etwa $= Q_1 b_h$ sein. Wenn also das System $1, b_1, b_2 \ldots b_{\nu_1-1}$ mit B bezeichnet wird, so lässt sich nach der Methode der Composition der Theile die Relation (11) so schreiben:

(12) $$Q_1 B\, Q_1 B = Q_1 B,$$

und so besagt sie nach §. 4, 1., dass die in

(13) $$Q = Q_1 B$$

enthaltenen Elemente von P eine Gruppe bilden, die die Gruppe Q_1 als Theiler enthält und selbst ein Theiler von P ist. Dass Q_1 Normaltheiler von Q ist, folgt aus §. 4, 5., weil Q_1 als Normal-

theiler von P vorausgesetzt ist, und aus der Darstellung (10) der Gruppe M ergiebt sich, dass $M = Q/Q_1$ ist.

Es ist noch zu zeigen, dass, wenn M Normaltheiler von P/Q_1 ist, auch Q Normaltheiler von P ist. Dies folgt so:

Ist e irgend ein Element in P und $Q_1 b_k$ ein Element in M, so folgt aus der Annahme, dass M Normaltheiler von P/Q_1 ist:

$$Q_1 e^{-1} Q_1 b_k Q_1 e = Q_1 b_k,$$

was wir auch nach der Composition der Theile durch die Formel

(14) $$Q_1 e^{-1} Q_1 B Q_1 e = Q_1 B$$

ausdrücken können. Da nun Q_1 Normaltheiler von P ist, so kann Q_1 mit jedem der anderen Factoren vertauscht werden, so dass aus (14) folgt:

$$e^{-1} Q_1 B e = Q_1 B,$$

oder

(15) $$e^{-1} Q e = Q,$$

wodurch ausgedrückt ist, dass Q Normaltheiler von P ist.

Aus dem Theorem 1. und 2. ergiebt sich das Corollar:

3. Ein Normaltheiler Q von P ist dann und nur dann ein grösster Normaltheiler, wenn die complementäre Gruppe P/Q einfach ist.

Wenn Q und Q' zwei Normaltheiler von P sind, so ist auch das symbolische Product $Q Q'$ ein Normaltheiler.

Denn es ist, weil Q ein Normaltheiler ist

$$Q Q' = Q' Q,$$

also

$$Q Q' Q Q' = Q Q Q' Q' = Q Q',$$

und dies ist nach §. 4, 1. das Kennzeichen, dass $Q Q'$ eine Gruppe ist. Dass es ein Normaltheiler von P ist, ergiebt sich dann ebenfalls nach §. 4, 2. aus

$$Q Q' B = Q B Q' = B Q Q',$$

wenn B irgend ein Theil von P ist.

Ist nun Q ein grösster Normaltheiler von P, und Q' von Q verschieden, so ist $Q Q'$ ein Normaltheiler von P, der sowohl Q als Q' in sich enthält und also von Q verschieden ist. Folglich ist, da es über Q keinen Normaltheiler von P giebt, ausser P selbst,

(16) $$Q Q' = P,$$

und ebenso muss auch

(17) $$Q' Q = P$$

sein. Diese Sätze gelten, wenn nur eine der beiden Gruppen Q, Q' grösster Normaltheiler von P ist. Wir nehmen jetzt an, dass sie beide diese Eigenschaft haben, und verstehen unter R den grössten gemeinschaftlichen Theiler von Q und Q'. Diese Gruppe R ist dann ein Normaltheiler von P sowohl als von Q und Q'. Denn ist a irgend ein Element in P, und c in Q sowohl als in Q' enthalten, so ist auch $a^{-1}ca$ in Q und in Q', also auch in R enthalten. Also ist $a^{-1}Ra = R$, und R ist Normaltheiler von P und mithin Normaltheiler von Q und von Q' (§. 4, 5.). Um Q in die Nebengruppen von R zu zerlegen, wählen wir ein passendes System von Elementen $1, b_1, b_2, b_3 \ldots$ in Q, so dass $R, Rb_1, Rb_2, Rb_3 \ldots$ alle von einander verschieden werden und setzen

$$Q = R + Rb_1 + Rb_2 + Rb_3 + \ldots,$$

was wir auch, wenn wir

(18) $$B = 1, b_1, b_2, b_3 \ldots$$

setzen, kurz mit

(19) $$Q = RB$$

bezeichnen können. Nun ist nach (13) $Q'Q = P$, also auch

(20) $$P = Q'RB = Q'B$$

oder

$$P = Q' + Q'b_1 + Q'b_2 + Q'b_3 \ldots$$

Die Nebengruppen

(21) $$Q', Q'b_1, Q'b_2, Q'b_3 \ldots$$

sind aber alle von einander verschieden. Denn wäre etwa

$$Q'b_2 = Q'b_1,$$

so würde folgen, da Q' die Einheit enthält, dass es ein Element e in Q' giebt, so dass

$$b_2 = eb_1$$

wäre. Dies Element e ist aber gleich $b_2 b_1^{-1}$, und also, da die b in Q enthalten sind, gleichfalls in Q und also auch in R enthalten. Dann aber wäre auch $Rb_2 = Rb_1$, was gegen die Voraussetzung ist.

Hiernach können wir die Elemente der zu R complementären Gruppe in Bezug auf Q und der zu Q' complementären Gruppe in Bezug auf P bilden. Wir erhalten diese beiden Gruppen

(22) $$\begin{aligned} Q/R &= R, Rb_1, Rb_2, Rb_3 \ldots \\ P/Q' &= Q', Q'b_1, Q'b_2, Q'b_3 \ldots \end{aligned}$$

Daraus aber erkennt man leicht, dass diese Gruppen nicht nur von gleichem Grade sind, sondern dass sie **isomorph** sind. Denn es ist gleichzeitig

$$R b_1\ R b_2 = R b_1 b_2$$

und

$$Q' b_1\, Q' b_2 = Q' b_1 b_2.$$

Ebenso kann man auch schliessen, dass die beiden Gruppen

$$Q'/R, \quad P/Q$$

isomorph sind.

Die Gruppen P/Q und P/Q' sind aber, da Q, Q' grösste Normaltheiler sind, nach 3) einfach, und folglich sind auch die damit isomorphen Gruppen Q'/R und Q/R einfach, und folglich haben wir den Satz:

4. Sind Q und Q' zwei verschiedene grösste Normaltheiler von P und ist R der Durchschnitt von Q und Q', so ist R grösster Normaltheiler sowohl von Q als von Q', und der Index von R in Bezug auf Q ist gleich dem Index von Q' in Bezug auf P.

Damit haben wir die Grundlage gewonnen, um sehr einfach den Satz von der Constanz der Indexreihe nachzuweisen.

Wir schreiben zur besseren Uebersicht die verschiedenen in Vergleich zu ziehenden Compositionsreihen so, dass wir den Index eines jeden Gliedes in Bezug auf das vorangehende unter das Glied setzen.

Danach mögen irgend zwei gegebene Compositionsreihen von P mit den zugehörigen Indices folgende sein:

$$\begin{array}{llllll} P, & Q, & Q_1, & Q_2, & Q_3 & \ldots \\ & \nu, & \nu_1, & \nu_2, & \nu_3 & \ldots \end{array} \tag{23}$$

$$\begin{array}{llllll} P, & Q', & Q'_1, & Q'_2, & Q'_3 & \ldots \\ & \nu', & \nu'_1, & \nu'_2, & \nu'_3 & \ldots \end{array} \tag{24}$$

Es sei nun R der Durchschnitt von Q und Q', und μ und μ' seien die Indices von R in Bezug auf Q und Q'. Wegen des Isomorphismus der Gruppen P/Q und Q'/R ist dann $\mu' = \nu$, und aus dem entsprechenden Grunde $\mu = \nu'$. Wir bilden eine Compositionsreihe von R mit der zugehörigen Indexreihe

$$\begin{array}{lllll} R, & R_1, & R_2, & R_3 & \ldots \\ & \mu_1, & \mu_2, & \mu_3 & \ldots, \end{array} \tag{25}$$

und da nun R ein grösster Normaltheiler von Q und von Q' ist, so können wir daraus zwei neue Compositionsreihen von P bilden, nämlich

$$(26)\qquad \begin{array}{l} P,\ Q,\ R,\ R_1,\ R_2,\ R_3 \ldots \\ \quad \nu,\ \nu',\ \mu_1,\ \mu_2,\ \mu_3 \ldots \end{array}$$

$$(27)\qquad \begin{array}{l} P,\ Q',\ R,\ R_1,\ R_2,\ R_3 \ldots \\ \quad \nu',\ \nu,\ \mu_1,\ \mu_2,\ \mu_3 \ldots \end{array}$$

Die beiden Compositionsreihen (26) und (27) von P haben also dieselbe Indexreihe.

Nehmen wir jetzt an, der zu beweisende Satz sei bereits als richtig erwiesen für Gruppen, deren Grad $\overline{\gtrless} \frac{1}{2} n$ ist (wenn n den Grad von P bedeutet), so folgt, dass alle Indexreihen von Q, dessen Grad ja ein echter Theiler von n und also höchstens $= \frac{1}{2} n$ ist, mit einander übereinstimmen, dass also die Reihen

$$\begin{array}{l} \nu',\ \mu_1,\ \mu_2,\ \mu_3 \ldots \\ \nu_1,\ \nu_2,\ \nu_3,\ \nu_4 \ldots, \end{array}$$

von der Anordnung abgesehen, übereinstimmen. Ebenso stimmen die Indexreihen von Q'

$$\begin{array}{l} \nu,\ \mu_1,\ \mu_2,\ \mu_3 \ldots \\ \nu_1',\ \nu_2',\ \nu_3',\ \nu_4' \ldots \end{array}$$

überein. Also stimmen auch die beiden Indexreihen von P

$$\begin{array}{l} \nu,\ \nu_1,\ \nu_2,\ \nu_3,\ \nu_4 \ldots \\ \nu',\ \nu_1',\ \nu_2',\ \nu_3',\ \nu_4' \ldots \end{array}$$

mit einander überein, da die erste mit $\nu, \nu', \mu_1, \mu_2, \mu_3 \ldots$, die zweite mit $\nu', \nu, \mu_1, \mu_2, \mu_3 \ldots$ übereinstimmt.

Für Gruppen vom Grade 2, die nur den einen Normaltheiler 1 haben, ist aber der Satz evident, und also ist er durch vollständige Induction allgemein bewiesen.

Wenn in zwei Compositionsreihen von P, die wir mit ihren Indexreihen jetzt so darstellen wollen

$$(28)\qquad \begin{array}{l} P,\ P_1,\ P_2,\ P_3 \ldots P_{\mu-1},\ 1 \\ \quad j_1,\ j_2,\ j_3 \ldots j_{\mu-1},\ j_\mu \end{array}$$

$$(29)\qquad \begin{array}{l} P,\ P_1',\ P_2',\ P_3' \ldots P_{\mu-1}',\ 1 \\ \quad j_1',\ j_2',\ j_3' \ldots j_{\mu-1}',\ j_\mu' \end{array}$$

ein gemeinschaftliches Glied $P_r = P_s'$ vorkommt, so gilt der Satz von der Constanz der Indexreihen auch für die Gruppe $P_r = P_s'$, und daraus folgt zunächst, dass $s = r$ sein muss, und

dass die Indexreihen $j_{r+1}, j_{r+2} \ldots j_\mu$ und $j'_{r+1}, j'_{r+2} \ldots j'_\mu$, von der Ordnung abgesehen, übereinstimmen. Folglich müssen auch die vorangehenden Theile der Indexreihen

$$j_1, j_2 \ldots j_r \text{ und } j'_1, j'_2 \ldots j'_r$$

übereinstimmen.

§. 7.

Weitere Sätze über die Compositionsreihen.

Von den Compositionsreihen gelten noch mannigfaltige Sätze, von denen wir hier noch die wichtigsten ableiten.

II. Ist P_ν irgend ein Normaltheiler von P, so giebt es eine Compositionsreihe von P, in der P_ν vorkommt.

Ist P_ν ein grösster Normaltheiler von P, so können wir $P_\nu = P_1$ setzen und die Compositionsreihe von da an beliebig fortsetzen. Ist aber P_ν kein grösster Normaltheiler von P, so suchen wir einen grössten Normaltheiler über P_ν, den wir mit P_1 bezeichnen. Dann ist P_ν ein Normaltheiler von P_1. Ist es ein grösster, so setzen wir $P_\nu = P_2$ und setzen von da die Compositionsreihe beliebig fort. Ist aber P_ν noch kein grösster Normaltheiler von P_1, so suchen wir einen grössten Normaltheiler von P_1 über P_ν und fahren so fort, bis wir schliesslich zu P_ν gelangen, was nach einer endlichen Anzahl von Schritten nothwendig eintreten muss. Wenn wir dann eine Compositionsreihe von P_ν anhängen, so haben wir eine Compositionsreihe von P, in der P_ν vorkommt, wie es der Satz II. verlangt.

In einer Compositionsreihe einer Gruppe P ist, vermöge der Definition, jedes Glied ein Normaltheiler jedes vorangehenden. Das erste Glied P_1 und das letzte Glied 1 sind zugleich Normaltheiler von P selbst. Bei den zwischenliegenden $P_2, P_3 \ldots$ wird dies im Allgemeinen nicht der Fall sein. In der Compositionsreihe giebt es also gewisse ausgezeichnete Glieder, die zugleich Normaltheiler von P selbst sind, die eine besondere Rolle spielen [1]). Hierüber leiten wir im Folgenden noch einen wichtigen Satz ab.

Angenommen, es sei Q ein Glied einer Compositionsreihe von P, das zugleich Normaltheiler von P ist, während das auf Q

[1]) Sie bilden die sogenannte Hauptreihe von P (Netto).

folgende Glied Q_1 nicht Normaltheiler von P ist. Dann giebt es unter den nach P conjugirten Gruppen $a^{-1} Q_1 a$ mehrere verschiedene, die wir mit

(1) $$Q_1, Q_1', Q_1'', Q_1''' \dots$$

bezeichnen wollen. Der grösste gemeinschaftliche Theiler R aller dieser Gruppen ist wieder Normaltheiler von P.

Nun sind aber alle die Gruppen (1) grösste Normaltheiler von Q, wie sich nach dem Schlusssatze des §. 3 daraus ergiebt, dass Q, Q_1 mit $a^{-1} Q a$, $a^{-1} Q_1 a$ isomorph sind, während Q als Normaltheiler von P mit $a^{-1} Q a$ identisch ist. Wir können also in der Compositionsreihe auf Q jede der Gruppen (1) folgen lassen, die alle denselben Index ν haben.

Ist nun Q_2 der grösste gemeinschaftliche Theiler von Q_1, Q_1' (also von Q_1 verschieden), so ist Q_2 nach dem Satze §. 6, 4. ein grösster Normaltheiler von Q_1 und Q_1', dessen Index gleichfalls ν ist. Also können wir die Compositionsreihe von Q an auf die folgenden beiden Arten fortsetzen:

(2) $$\underset{\nu}{Q,\ Q_1,}\ \underset{\nu}{Q_2,} \qquad \underset{\nu}{Q\ Q_1'}\ \underset{\nu}{Q_2}$$

Das hierin ausgedrückte Gesetz wollen wir nun verallgemeinern und durch vollständige Induction beweisen.

Wenn Q_2 noch nicht gleich R ist, so fügen wir zu Q_1, Q_1' eine dritte Gruppe Q_1'' aus der Reihe (1) hinzu, so dass der Durchschnitt Q_3 von Q_1, Q_1', Q_1'' ein echter Theiler von Q_2 wird, und fahren so fort, bis wir zum grössten gemeinschaftlichen Theiler R aller Gruppen (1) gelangt sind.

Es sei also:

(3)
$$\begin{array}{llll} Q_2 & \text{der Durchschnitt} & \text{von} & Q_1, Q_1' \\ Q_3 & \quad " & \quad " & Q_1, Q_1', Q_1'' \\ \dots & \dots & \dots & \dots \\ Q_r & \quad " & \quad " & Q_1, Q_1', Q_1'' \dots Q_1^{(r-1)} \end{array}$$

und die Anordnung der Gruppen $Q_1, Q_1' \dots Q_1^{(r-1)}$ sei so gewählt, dass von den Gruppen $Q_1, Q_2 \dots Q_r$ jede ein echter Theiler der vorangehenden ist. Diese Anordnung lässt sich fortsetzen, so lange Q_r nicht gleich R ist.

Wir wollen beweisen, dass wir die Compositionsreihe von P so wählen können, dass darin

(4) $$\underset{\nu}{Q,\ Q_1,}\ \underset{\nu}{Q_2} \dots \underset{\nu}{Q_r}$$

vorkommt, und dass die Indices in diesem Theile der Reihe alle gleich ν sind.

Die Behauptung ist richtig für $r = 2$, und wir beweisen sie allgemein durch vollständige Induction, unter der Voraussetzung, dass sie für r schon als richtig erwiesen sei.

Ist Q_r nicht gleich R, so wählen wir $Q_1^{(r)}$ so, dass Q_{r+1} der Durchschnitt von $Q_1, Q_1' \ldots Q_1^{(r-1)}, Q_1^{(r)}$ ist, und bezeichnen überdies den Durchschnitt von $Q_1, Q_1' \ldots Q_1^{(r-2)}, Q_1^{(r)}$ mit Q_r'. Dann ist Q_r' von Q_r verschieden und Q_{r+1} ist der Durchschnitt von Q_r und Q_r'. Nun haben wir nach der Voraussetzung (4) zwei entsprechende Stücke der Compositionsreihe mit der constanten Indexreihe ν

$$(5) \qquad \begin{array}{l} Q, Q_1 \ldots Q_{r-1}\, Q_r, \\ Q, Q_1 \ldots Q_{r-1}\, Q_r'; \end{array}$$

denn die zweite dieser Reihen ist genau wie die erste nach der Vorschrift (3) gebildet, nur dass $Q_1^{(r)}$ an Stelle von $Q_1^{(r-1)}$ getreten ist. Nach dem Satze §. 6, 2. ist daher Q_{r+1} grösster Normaltheiler sowohl von Q_r als von Q_r', und zwar vom Index ν, und es folgt also, was bewiesen werden sollte, dass die Compositionsreihe so fortgesetzt werden kann:

$$(6) \qquad Q, Q_1 \ldots Q_{r-1}, Q_r, Q_{r+1},$$

und dass der neu hinzugekommene Index gleichfalls ν ist.

Dies können wir nun fortsetzen, bis wir zur Gruppe R gelangt sind, und erhalten ein Stück der Compositionsreihe

$$(7) \qquad \begin{array}{l} Q, Q_1, Q_2 \ldots R, \\ \quad\;\; \nu \quad \nu \qquad \nu \end{array}$$

deren letztes Glied R wieder Normaltheiler von P ist und in der alle Indices übereinstimmen.

Setzen wir von R an die Compositionsreihe fort, so kann sich der Index ändern; er kann aber von da an wieder gleich gehalten werden, bis man abermals zu einem Normaltheiler von P gelangt.

Damit ist der folgende Satz bewiesen:

III. Man kann die Compositionsreihe von P mit ihrer Indexreihe

$$(8) \qquad \begin{array}{l} P, P_1, P_2, P_3 \ldots \\ \quad\; j_1, j_2, j_3 \ldots \end{array}$$

so anordnen, dass, so oft eine Aenderung in der Indexreihe eintritt, also j_{r+1} von j_r verschieden ist, P_r ein Normaltheiler von P ist.

§. 8.

Metacyklische Gruppen.

Wir haben in §. 176 des ersten Bandes bei den Permutationsgruppen metacyklische Gruppen definirt und ihre Bedeutung für die Auflösung der Gleichungen kennen gelernt. Der Begriff ist aber von der besonderen Bedeutung der Gruppenelemente unabhängig, und wir definiren daher jetzt allgemein:

Eine Gruppe, deren Indexreihe aus lauter Primzahlen besteht, soll eine metacyklische Gruppe heissen.

Für diese Gruppen gilt ein für die Anwendungen auf die Algebra wichtiger Satz, der aber von diesen Anwendungen unabhängig ist und den wir daher hier noch ableiten. Der Satz lautet:

IV. Eine metacyklische Gruppe hat einen von der Einheitsgruppe verschiedenen commutativen Normaltheiler[1]).

Ist P eine metacyklische Gruppe und

$$(1) \qquad \begin{matrix} P, & P_1, & P_2 & \ldots & P_{\mu-1}, & 1 \\ & \dot{j}_1, & \dot{j}_2 & \ldots & \dot{j}_{\mu-1}, & \dot{j}_\mu \end{matrix}$$

die Compositionsreihe, deren Indexreihe $j_1, j_2 \ldots$ aus lauter Primzahlen besteht, so ist $P_{\mu-1}$ jedenfalls eine commutative Gruppe; denn wenn π irgend ein von 1 verschiedenes Element aus $P_{\mu-1}$ ist, so sind die Potenzen

$$(2) \qquad 1, \pi, \pi^2 \ldots \pi^{j_\mu - 1}$$

(weil j_μ eine Primzahl ist) alle von einander verschieden und machen also die ganze Gruppe $P_{\mu-1}$ aus; die cyklische Gruppe (2) ist aber gewiss commutativ, weil für je zwei Exponenten h, k immer

$$\pi^h \pi^k = \pi^k \pi^h = \pi^{h+k}$$

ist. Zugleich ist, nach der Definition der Compositionsreihe. $P_{\mu-1}$ Normaltheiler von $P_{\mu-2}$.

Wir nehmen demnach jetzt an, wir haben einen von der Einheit verschiedenen commutativen Normaltheiler Q_ν irgend einer Gruppe P_ν der Reihe (1) und setzen ausserdem noch voraus,

---

[1]) C. Jordan, Traité des substitutions, Livre IV.

wenn es zu P_ν mehrere Theiler von der Beschaffenheit wie Q_ν giebt, dass einer von möglichst niedrigem Grade für Q_ν genommen ist.

Wenn wir dann nachweisen, wie man aus Q_ν einen commutativen Normaltheiler $Q_{\nu-1}$ von $P_{\nu-1}$ ableiten kann, der zugleich Q_ν enthält, so können wir dies Verfahren fortsetzen, bis wir zu einem commutativen Normaltheiler Q von P selbst gelangt sind, wie ihn unser Satz verlangt.

Wählen wir irgend ein Element γ in der Gruppe $P_{\nu-1}$, welches nicht in P_ν enthalten ist, so ist, da P_ν ein Normaltheiler von $P_{\nu-1}$ ist,

(3) $$\gamma P_\nu = P_\nu \gamma,$$

und wenn daher h der niedrigste Exponent ist, für den γ^h in P_ν enthalten ist, so ist h grösser als 1 und

(4) $$\gamma^h P_\nu = P_\nu,$$

und die in dem System der Nebengruppen

(5) $$P_\nu, \ \gamma P_\nu, \ \gamma^2 P_\nu \ldots \ \gamma^{h-1} P_\nu$$

enthaltenen Elemente, die alle von einander verschieden sind, bilden eine Gruppe, deren Grad, wenn der Grad von P_ν mit p_ν bezeichnet wird, gleich $h p_\nu$ ist. Die Gruppe (5) ist aber auch ein Theiler von $P_{\nu-1}$ und folglich muss $h p_\nu$ ein Theiler von $p_{\nu-1} = j_\nu p_\nu$ sein, und h ist ein Theiler von j_ν. Da aber j_ν eine Primzahl ist, so muss $h = j_\nu$ sein, und durch (5) ist die ganze Gruppe $P_{\nu-1}$ erschöpft:

(6) $$P_{\nu-1} = P_\nu + \gamma P_\nu + \gamma^2 P_\nu + \cdots \gamma^{j_\nu - 1} P_\nu.$$

Wir betrachten nun das System der transformirten Gruppen

(7) $$\gamma^{-1} Q_\nu \gamma,$$

worin γ alle Elemente von $P_{\nu-1}$ durchläuft.

Diese Gruppen sind alle mit einander isomorph und sind also ebenso wie Q_ν commutativ. Sie sind alle in P_ν enthalten, und sind, da $\gamma^{-1} P_\nu \gamma = P_\nu$ ist, nach dem Schlusssatze von §. 3 Normaltheiler von P_ν.

Wenn alle Gruppen (7) mit einander identisch sind, so ist Q_ν Normaltheiler von $P_{\nu-1}$, und wir erreichen unseren Zweck der Bestimmung von $Q_{\nu-1}$ schon dadurch, dass wir Q_ν selbst, oder, falls noch ein commutativer Normaltheiler niedrigeren Grades von $P_{\nu-1}$ vorhanden sein sollte, diesen letzteren, für $Q_{\nu-1}$ nehmen.

Im anderen Falle wollen wir die von einander verschiedenen der Gruppen (7) mit

(8) $$Q_\nu, Q'_\nu, Q''_\nu \ldots$$

bezeichnen, und daraus eine Gruppe

(9) $$R = (Q_\nu, Q'_\nu, Q''_\nu \ldots)$$

ableiten, die dadurch definirt sein soll, dass es die kleinste Gruppe ist, die jede der Gruppen (8) als Theiler enthält, und die wir als das kleinste gemeinschaftliche Vielfache der Gruppen $Q_\nu, Q'_\nu, Q''_\nu \ldots$ bezeichnen können.

Dass es eine und nur eine solche Gruppe R giebt, und dass jede Gruppe, die durch $Q_\nu, Q'_\nu, Q''_\nu \ldots$ theilbar ist, auch durch R theilbar sein muss, ist leicht einzusehen. Denn erstens giebt es endliche Gruppen, z. B. die Gruppe P_ν, die alle Gruppen (8) als Theiler enthalten, und zweitens, wenn zwei Gruppen R, R' alle diese Gruppen enthalten, so gilt dasselbe auch von dem Durchschnitt von R und R'. Ist daher R von möglichst niedrigem Grade, so muss dieser Durchschnitt mit R identisch sein, und R ist also ein Theiler von R'. Wenn R' auch von möglichst niedrigem Grade ist, so ist R' von R nicht verschieden.

Von dieser Gruppe R weisen wir nun nach:

a) dass sie ein Normaltheiler von $P_{\nu-1}$ ist,

b) dass sie eine commutative Gruppe ist.

Wenn wir dies Beides nachgewiesen haben, so sind wir am Ziele; denn dann können wir, wenn es nicht noch einen commutativen Normaltheiler niedrigeren Grades von $P_{\nu-1}$ giebt, R selbst für $Q_{\nu-1}$ wählen.

Das Erste ist aber ohne Weiteres klar. Denn bedeutet γ irgend ein Element aus $P_{\nu-1}$, so ist

$$\gamma^{-1} R \gamma = (\gamma^{-1} Q_\nu \gamma, \gamma^{-1} Q'_\nu \gamma, \gamma^{-1} Q''_\nu \gamma \ldots)$$

das kleinste gemeinschaftliche Vielfache der Gruppen

$$\gamma^{-1} Q_\nu \gamma, \gamma^{-1} Q'_\nu \gamma, \gamma^{-1} Q''_\nu \gamma \ldots$$

Diese Gruppen aber sind nach der Definition (7) in ihrer Gesammtheit von den Gruppen

$$Q_\nu, Q'_\nu, Q''_\nu \ldots$$

nicht verschieden, und folglich ist

$$\gamma^{-1} R \gamma = R,$$

d. h. R ist Normaltheiler von $P_{\nu-1}$.

Um aber nachzuweisen, dass R eine commutative Gruppe ist, müssen wir zwei Hülfsbetrachtungen voranschicken.

1) Es ist zu beweisen, dass irgend zwei der Gruppen $Q_\nu, Q'_\nu, Q''_\nu \ldots$ ausser der Einheit keinen gemeinschaftlichen Theiler haben.

Wir brauchen hierzu nur nachzuweisen, dass Q_ν, Q'_ν diese Eigenschaft haben. Denn haben

$$Q'_\nu = \gamma'^{-1} Q_\nu \gamma', \quad Q''_\nu = \gamma''^{-1} Q_\nu \gamma''$$

den grössten gemeinschaftlichen Theiler T, so haben Q_ν und $Q'''_\nu = \gamma' Q''_\nu \gamma'^{-1}$ den grössten gemeinschaftlichen Theiler $\gamma' T \gamma'^{-1}$.

Nehmen wir also an, es sei T der grösste gemeinschaftliche Theiler von Q_ν und Q'_ν, so ist T gewiss eine commutative Gruppe, weil Q_ν, Q'_ν solche sind. Es ist aber T auch Normaltheiler von P_ν. Denn Q_ν und Q'_ν sind solche Theiler; und wenn also τ ein Element aus T und π ein Element aus P_ν ist, so ist $\pi^{-1}\tau\pi$ sowohl in Q_ν als in Q'_ν, also auch in T enthalten. Folglich ist $\pi^{-1} T \pi = T$.

Nun haben wir aber angenommen, dass Q_ν ein commutativer Normaltheiler von P_ν über der Einheit von möglichst niedrigem Grade sei; ferner waren Q_ν und Q'_ν von einander verschieden. Also kann T nur die Einheitsgruppe selbst sein, w. z. b. w.

2) Um die Gruppe R zu bilden, können wir so verfahren, dass wir die Elemente von Q_ν, Q'_ν, $Q''_\nu \ldots$ in beliebiger Reihenfolge und Wiederholung so lange mit einander componiren, als noch neue Elemente entstehen. Denn alle so gebildeten Zusammensetzungen bilden eine Gruppe C, die in R enthalten ist, weil R die einzelnen Elemente von Q_ν, Q'_ν, $Q''_\nu \ldots$ enthält. Andererseits sind auch die Gruppen Q_ν, Q'_ν, $Q''_\nu \ldots$ in C enthalten, und folglich ist R in C enthalten und C ist mit R identisch.

Um also endlich zu beweisen, dass R eine commutative Gruppe ist, bleibt uns nur zu zeigen, dass, wenn α, β irgend zwei Elemente aus Q_ν, Q'_ν, $Q''_\nu \ldots$ sind, die Vertauschbarkeit

$$(10) \qquad \alpha\beta = \beta\alpha$$

besteht.

Wenn nun α, β beide in dieselbe Gruppe Q_ν gehören, so ist (10) Folge unserer Annahme, dass Q_ν commutativ sei; und ebenso ist es, wenn beide in einer der anderen Gruppen Q'_ν, $Q''_\nu \ldots$ vorkommen.

Sind aber α und β in zwei verschiedenen Gruppen, etwa in Q_ν und Q'_ν enthalten, so schliessen wir so: Weil β in P_ν enthalten und Q_ν ein Normaltheiler von P_ν ist, so ist auch

(11) $$\beta^{-1}\alpha\beta = \alpha'$$

in Q_ν enthalten. Daraus folgt:

(12) $$\beta\alpha'\alpha^{-1} = \alpha\beta\alpha^{-1} = \beta',$$

und weil α in P_ν enthalten und Q'_ν ein Normaltheiler von P_ν ist, so ist auch β' in Q'_ν enthalten. Aus (12) aber folgt

$$\alpha'\alpha^{-1} = \beta^{-1}\beta' = \delta,$$

und demnach ist das Element δ sowohl in Q_ν als in Q'_ν enthalten. Es kann also nach dem, was unter 1) bewiesen ist, nur das Einheitselement sein, d. h. es ist

$$\alpha' = \alpha, \quad \beta' = \beta,$$

und demnach folgt aus (11), dass $\alpha\beta = \beta\alpha$ sein muss, wie bewiesen werden sollte.

Zweiter Abschnitt.

Abel'sche Gruppen.

---

§. 9.

Darstellung Abel'scher Gruppen durch eine Basis.

Wir haben schon in §. 1 solche Gruppen, in denen bei der Composition das commutative Gesetz gilt, commutative oder Abel'sche Gruppen genannt. Bei diesen Gruppen, die in den Anwendungen von besonderer Wichtigkeit sind, herrschen viel einfachere Gesetze, als in den allgemeinen Gruppen, wie wir jetzt sehen werden. Es gelten für die Zusammensetzung der Elemente in diesen Gruppen dieselben Regeln, wie bei der Multiplication von Zahlen, und wir nennen demnach die Composita von Elementen einer solchen Gruppe, wie bei der Multiplication, Producte und Potenzen.

Auch hier beschränken wir uns auf die Betrachtung endlicher Gruppen.

Aus der Definition der Abel'schen Gruppen folgt, dass das commutative Gesetz auch bei der Composition der Theile einer solchen Gruppe gilt (§. 4). Jeder Theiler einer Abel'schen Gruppe ist selbst eine Abel'sche Gruppe, und ist zugleich Normaltheiler, so dass wir bei diesen Gruppen den Zusatz „Normal" weglassen können.

Eine Gruppe, die nur aus den Wiederholungen eines Elementes besteht, wie

$$1, A, A^2 \ldots A^{a-1},$$

haben wir schon früher (Bd. I, §. 148) eine cyklische Gruppe genannt, und wir behalten diese Bezeichnung hier bei. Wenn a die kleinste positive Zahl ist, für die $A^a = 1$ ist, also a der Grad der Gruppe, so heisst a auch der Grad des Elementes A. Ist m irgend ein Exponent, für den $A^m = 1$ ist, so ist m ein

Vielfaches von a. Das Element 1 hat den Grad 1. Alle cyklischen Gruppen sind commutativ.

Es gilt nun für jede Abel'sche Gruppe S der Fundamentalsatz, dass sich immer ein System von Elementen $A, B, C \ldots$ von den Graden $a, b, c \ldots$ so auswählen lässt, dass sich in der Form

$$\Theta = A^\alpha B^\beta C^\gamma \ldots$$

jedes Element Θ von S, und jedes nur einmal, darstellen lässt, wenn α ein volles Restsystem nach dem Modul a, β ein volles Restsystem nach dem Modul b, γ ein volles Restsystem nach dem Modul c etc. durchläuft.

Ein System von Elementen, das zu einer solchen Darstellung geeignet ist, heisst eine Basis der Gruppe, und wir können den zu beweisenden Satz demnach so aussprechen:

I. Jede Abel'sche Gruppe lässt sich durch eine Basis darstellen.

Der Beweis des Satzes gründet sich auf folgende Reihe von Schlüssen:

1. Ist n der Grad der Gruppe S, sind $A_1, A_2 \ldots A_n$ ihre Elemente und $a_1, a_2 \ldots a_n$ deren Grade; durchlaufen ferner $\alpha_1, \alpha_2 \ldots \alpha_n$ volle Restsysteme nach den Moduln $a_1, a_2 \ldots a_n$, so wird in der Form

(1) $$\Theta = A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_n^{\alpha_n}$$

jedes Element von S und jedes gleich oft dargestellt.

Dass man jedes Element in der Form (1) überhaupt erhält, sieht man unmittelbar; denn man erhält z. B. A_1, wenn man $\alpha_1 = 1, \alpha_2 = 0 \ldots \alpha_n = 0$ setzt.

Es ist noch zu beweisen, dass man jedes Element gleich oft erhält.

Wenn aber

(2) $$1 = A_1^{h_1} A_2^{h_2} \ldots A_n^{h_n}$$

eine Darstellung des Elementes 1 ist, so ändert sich Θ nicht, wenn man $\alpha_1, \alpha_2 \ldots \alpha_n$ in (1) durch $\alpha_1 + h_1, \alpha_2 + h_2 \ldots \alpha_n + h_n$ ersetzt. Es wird also jedes Element Θ durch (1) mindestens so oft dargestellt, als das Element 1 durch (2).

Geben andererseits die beiden Exponentenreihen $\alpha_1, \alpha_2 \ldots \alpha_n$ und $\alpha_1', \alpha_2' \ldots \alpha_n'$ zwei Darstellungen des Elementes Θ, so hat man

(3) $$1 = A_1^{\alpha_1' - \alpha_1} A_2^{\alpha_2' - \alpha_2} \dots A_n^{\alpha_n' - \alpha_n},$$

also eine Darstellung des Elementes 1. Also können wir nach (2) setzen:

$$\alpha_1' = \alpha_1 + h_1, \ \alpha_2' = \alpha_2 + h_2 \dots \alpha_n' = \alpha_n + h_n.$$

Es kann folglich auch nicht mehr verschiedene Darstellungen des Elementes Θ geben, als die Anzahl der Darstellungen des Elementes 1 beträgt. Wir bezeichnen die Anzahl dieser Darstellungen mit h. Im Ganzen ist aber die Anzahl der verschiedenen möglichen Bestimmungen der α in (1) gleich dem Producte $a_1 a_2 \dots a_n$, und da n die Anzahl der Elemente von S ist, so folgt

(4) $$n h = a_1 a_2 \dots a_n.$$

Aus der Formel (4) ergiebt sich der Satz:

2. Wenn r eine im Grade n der Gruppe aufgehende Primzahl ist, so giebt es in S ein Element vom Grade r.

Denn aus (4) sieht man zunächst, dass einer der Grade $a_1, a_2, \dots a_n$ durch r theilbar ist. Ist also etwa $a_1 = rk$, so ist A_1^k ein Element vom Grade r.

3. Sind $A, B \dots$ irgend welche Elemente in S von den Graden $a, b \dots$, so ist auch $AB \dots$ ein Element in S, und der Grad dieses Productes ist ein Theiler des kleinsten gemeinschaftlichen Vielfachen m von $a, b \dots$

Denn es ist

$$(AB \dots)^m = A^m B^m \dots = 1,$$

und folglich m ein Vielfaches des Grades von $AB \dots$

4. Ist der Grad n der Gruppe S in zwei Factoren $n = ab$ zerlegt, so dass a und b relativ prim sind, so giebt es in S genau a Elemente A, deren Grad ein Theiler von a ist, und b Elemente B, deren Grad ein Theiler von b ist, und in der Form

(5) $$\Theta = AB$$

sind sämmtliche Elemente von S und jedes nur einmal enthalten.

Um die Richtigkeit dieses Satzes einzusehen, stellen wir folgende Ueberlegung an. Der Inbegriff $\mathfrak{A}$ der Elemente A, deren

Grad ein Theiler von a ist, ist eine in S enthaltene Gruppe; denn sind A, A' zwei solche Elemente, so ist nach 3. der Grad von AA' ein Theiler von a, und AA' ist also auch in $\mathfrak{A}$ enthalten.

Ebenso ist der Inbegriff $\mathfrak{B}$ der Elemente B, deren Grad ein Theiler von b ist, eine Gruppe. Das Element 1 kommt sowohl in $\mathfrak{A}$ als in $\mathfrak{B}$ vor, sonst enthalten beide kein gemeinschaftliches Element.

Der Grad a' von $\mathfrak{A}$ ist relativ prim zu b. Denn ist r eine in a' aufgehende Primzahl, so giebt es nach 2. in $\mathfrak{A}$ ein Element vom Grade r. Da aber der Grad jedes Elementes von $\mathfrak{A}$ ein Theiler von a ist, so ist auch r ein Theiler von a und nicht von b.

Ebenso beweist man, dass der Grad b' von $\mathfrak{B}$ relativ prim zu a ist.

Nun bestimme man (nach Bd. I, §. 118) zwei ganze Zahlen x und y, so dass

(6) $$ax + by = 1$$

ist, und nehme irgend ein Element Θ von S. Dann ist

(7) $$\Theta = \Theta^{ax}\,\Theta^{by},$$

und nun ist, da $(\Theta^{by})^a = 1$ ist, Θ^{by} in $\mathfrak{A}$ und aus dem gleichen Grunde Θ^{ax} in $\mathfrak{B}$ enthalten. Also folgt aus (7):

(8) $$\Theta = AB.$$

Demnach ist jedes Element Θ in der Form AB enthalten. Eine solche Darstellung ist aber auch nur auf eine Art möglich. Denn sind A', B' zwei Elemente aus $\mathfrak{A}$ und $\mathfrak{B}$, und ist

$$AB = A'B',$$

so folgt, wenn man in die Potenz $by = 1 - ax$ erhebt, $A = A'$ und folglich auch $B = B'$. Die Anzahl der verschiedenen Producte der Form AB ist aber $= a'b'$, und daher hat man

$$n = ab = a'b',$$

und da a relativ prim zu b' und b relativ prim zu a' ist:

$$a' = a, \quad b' = b.$$

Damit ist der Satz 4. in allen seinen Theilen bewiesen.

Wenn nun die beiden Gruppen $\mathfrak{A}$, $\mathfrak{B}$ durch Basen dargestellt sind, so folgt aus der Formel (8), dass auch S durch eine Basis dargestellt ist, und die Basis von S enthält die Elemente der Basen von $\mathfrak{A}$ und $\mathfrak{B}$ und keine anderen.

Wenn a und b weiter in Factoren zerlegbar sind, die zu einander relativ prim sind, so können wir mit den Gruppen $\mathfrak{A}$ und $\mathfrak{B}$ wieder ebenso verfahren, und wir kommen also zu dem Resultate, dass unser Theorem I. allgemein bewiesen ist, wenn wir es noch für Gruppen nachweisen können, deren Grad eine Potenz einer Primzahl ist.

Es sei also jetzt der Grad n der Gruppe S eine Potenz einer Primzahl p

(9) $$n = p^k.$$

Die Grade aller Elemente von S, die ja Divisoren von n sind, müssen dann gleichfalls Potenzen von p sein. Es ist nachzuweisen, dass eine solche Gruppe durch eine Basis darstellbar ist.

Man wähle in S ein Element A von möglichst hohem Grade a. Dann ist a eine Potenz von p und die Grade aller anderen Elemente sind Theiler von a, so dass für jedes Element Θ von S

(10) $$\Theta^a = 1$$

ist. Die Elemente

(11) $$1, A, A^2 \ldots A^{a-1}$$

sind alle von einander verschieden, und ihre Gesammtheit ist ein Theiler von S. Ist damit die Gruppe S erschöpft, ist also jedes Element von der Form A^α, so ist S durch eine eingliedrige Basis dargestellt. Wenn aber S mit (11) noch nicht erschöpft ist, so wird es doch für jedes Element Θ von S einen gewissen Exponenten h geben, so dass Θ^h in der Reihe (11) enthalten ist. Gewiss wird das eintreten, wenn h der Grad von Θ, also $\Theta^h = 1$ ist. Unter diesen Zahlen h wird eine die kleinste positive sein, die wir mit b bezeichnen wollen. Es giebt also für jedes Element Θ eine gewisse kleinste positive Zahl b, so dass

(12) $$\Theta^b = A^\lambda$$

in der Reihe (11) enthalten ist.

Diese Zahl b ist ein Theiler von a, also auch eine Potenz von p und zugleich ein Theiler von λ. Denn setzen wir $a = qb + b'$, wo $0 \leqq b' < b$ ist, so folgt aus (10) und (12)

$$\Theta^a = A^{\lambda q}\, \Theta^{b'} = 1,$$

oder $\Theta^{b'} = A^{-\lambda q}$, und wenn also b' nicht Null ist, so giebt es gegen die Voraussetzung eine noch kleinere Zahl als b, nämlich b', die der Forderung (12) genügt.

Aus (12) folgt ferner

$$1 = \Theta^a = A^{\frac{\lambda a}{b}};$$

also muss $\lambda a : b$ ein Vielfaches von a und folglich λ ein Vielfaches von b sein. Wenn wir daher

(13) $$B = \Theta A^{-\frac{\lambda}{b}}$$

setzen, so ist $B^b = 1$, und zugleich ist B^b die niedrigste Potenz von B, die einer Potenz von A gleich wird, weil, wenn $B^{b'}$ eine Potenz von A ist, dasselbe nach (13) auch von $\Theta^{b'}$ gilt. Wir nehmen das Element Θ so gewählt an, dass b so gross als möglich wird. Dann ist auch für jedes andere Element Θ_1 aus S immer Θ_1^b eine Potenz von A, deren Exponent durch b theilbar ist.

Ist nun

$$\alpha = 0, 1, 2 \ldots a - 1$$
$$\beta = 0, 1, 2 \ldots b - 1,$$

so sind die Elemente

(14) $$A^\alpha B^\beta$$

in der Anzahl ab alle von einander verschieden. Sie bilden einen in S enthaltenen Theiler S', der durch die Basis A, B dargestellt ist. Ist S' mit S identisch, so sind wir am Ziele.

Ist aber S durch (14) noch nicht erschöpft, so fahren wir in derselben Weise fort.

Wir wollen durch Anwendung der vollständigen Induction gleich allgemein schliessen.

Es sei ein Theiler $S_{\nu-1}$ von S ermittelt, der durch eine Basis in der Form dargestellt ist

(15) $$S_{\nu-1} = A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_{\nu-1}^{\alpha_{\nu-1}},$$

von dem wir folgende Voraussetzungen machen:

1) Die Grade von $A_1, A_2 \ldots A_{\nu-1}$ seien $a_1, a_2 \ldots a_{\nu-1}$, und es sei

$$a_1 \geqq a_2 \geqq \ldots \geqq a_{\nu-1}.$$

2) Für jedes in S enthaltene Element Θ sei

(16) $$\Theta^{a_{\nu-1}} = A_1^{\lambda_1} A_2^{\lambda_2} \ldots A_{\nu-2}^{\lambda_{\nu-2}},$$

d. h. in $S_{\nu-2}$ enthalten, und die Exponenten $\lambda_1, \lambda_2 \ldots \lambda_{\nu-2}$ seien durch $a_{\nu-1}$ theilbar.

Die oben abgeleitete Gruppe S' genügt diesen Forderungen, wenn $\nu = 3$ und $a_{\nu-1} = b$ gesetzt wird, und es ist nun zu zeigen,

wie man, wenn $S_{\nu-1}$ noch nicht die ganze Gruppe S erschöpft, daraus eine eben solche umfassendere Gruppe S_ν ableiten kann.

Für jedes Element Θ von S wird es einen gewissen niedrigsten positiven Exponenten a_ν geben, für den Θ^{a_ν} in $S_{\nu-1}$ enthalten ist, und dies a_ν ist wegen (16) gleich oder kleiner als $a_{\nu-1}$, und ist ausserdem eine Potenz von p, da es ein Theiler des Grades von Θ sein muss. Wir wählen Θ so, dass der Exponent a_ν so gross als möglich wird. Ist Θ_1 ein beliebiges anderes Element in S, und Θ_1^h die niedrigste Potenz von Θ_1, die in $S_{\nu-1}$ enthalten ist, so ist auch h eine Potenz von p und gleich oder kleiner als a_ν. Es ist daher $\Theta_1^{a_\nu}$ in $S_{\nu-1}$ enthalten.

Setzen wir aber

(17) $$\Theta_1^{a_\nu} = A_1^{\lambda_1} A_2^{\lambda_2} \ldots A_{\nu-1}^{\lambda_{\nu-1}},$$

so sind die sämmtlichen Exponenten λ durch a_ν theilbar. Denn es ist

$$\Theta_1^{a_{\nu-1}} = A_1^{\frac{\lambda_1 a_{\nu-1}}{a_\nu}} A_2^{\frac{\lambda_2 a_{\nu-1}}{a_\nu}} \ldots A_{\nu-1}^{\frac{\lambda_{\nu-1} a_{\nu-1}}{a_\nu}},$$

und nach der Voraussetzung 2) müssen die Exponenten von $A_1, A_2 \ldots A_{\nu-1}$ auf der rechten Seite dieser Formel durch $a_{\nu-1}$ theilbare ganze Zahlen sein. Folglich sind $\lambda_1, \lambda_2 \ldots \lambda_{\nu-1}$ durch a_ν theilbar. Wir können also, indem wir zu dem oben betrachteten speciellen Θ zurückkehren und unter $h_1, h_2 \ldots h_{\nu-1}$ ganze Zahlen verstehen,

$$\Theta^{a_\nu} = A_1^{h_1 a_\nu} A_2^{h_2 a_\nu} \ldots A_{\nu-1}^{h_{\nu-1} a_\nu}$$

setzen, und wenn wir dann

$$A_\nu = \Theta A_1^{-h_1} A_2^{-h_2} \ldots A_{\nu-1}^{-h_{\nu-1}}$$

annehmen, so ist

(18) $$A_\nu^{a_\nu} = 1$$

die niedrigste Potenz von A_ν, die in $S_{\nu-1}$ enthalten ist (weil sonst auch noch eine niedrigere Potenz von Θ in $S_{\nu-1}$ enthalten wäre).

Dann ist

(19) $$A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_\nu^{\alpha_\nu}, \qquad \alpha_i = 0, 1, 2 \ldots a_i - 1$$

nur $= 1$, wenn $\alpha_1, \alpha_2 \ldots \alpha_\nu$ durch $a_1, a_2 \ldots a_\nu$ theilbar und folglich $= 0$ sind, und demnach sind die in (19) dargestellten Elemente alle von einander verschieden. Diese Elemente bilden aber eine Gruppe S_ν mit der Basis $A_1, A_2 \ldots A_\nu$, die der Forderung 1) genügt.

Zugleich ist, wie die Formel (17) zeigt, wenn Θ_1 ein beliebiges Element in S ist, $\Theta_1^{a_\nu}$ in $S_{\nu-1}$ enthalten, und die Exponenten $\lambda_1, \lambda_2 \ldots \lambda_{\nu-1}$ sind durch a_ν theilbar. Es ist daher auch die Forderung 2) befriedigt.

Damit ist also unser Satz I. bewiesen. Zugleich sehen wir aus dieser Ableitung, dass man für eine beliebige Abel'sche Gruppe S die Elemente der Basis immer so annehmen kann, dass ihre Grade Primzahlpotenzen sind.

Aus der Darstellbarkeit durch eine Basis folgt auch, dass jede Abel'sche Gruppe metacyklisch ist; denn sind die Elemente einer solchen Gruppe S in der Form dargestellt:

$$A = A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_\nu^{\alpha_\nu},$$

und ist p eine im Grade a_1 von A_1 aufgehende Primzahl, so bilden die Elemente

$$A' = A_1^{\alpha_1 p} A_2^{\alpha_2} \ldots A_\nu^{\alpha_\nu},$$

wenn α_1 ein volles Restsystem nach dem Modul $a_1 : p$ durchläuft, einen Theiler S' von S vom Index p, der durch die Basis $A_1^p, A_2 \ldots A_\nu$ darstellbar ist. Von S' kann man wieder auf die gleiche Weise einen Theiler von Primzahlindex finden u. s. f. Also ist S metacyklisch (§. 8).

§. 10.

Die Invarianten der Abel'schen Gruppen.

Der Beweis, den wir im vorigen Paragraphen für die Möglichkeit der Darstellung einer Abel'schen Gruppe durch eine Basis mitgetheilt haben, enthält zugleich einen Weg, eine solche Basis zu finden, und zwar eine, bei der die Grade der Basiselemente Primzahlpotenzen sind. Gleichwohl kann es vorkommen, dass eine und dieselbe Gruppe auf verschiedene Arten durch Basen dargestellt werden kann.

Betrachten wir z. B. zwei Elemente A, B, deren Grade a, b relativ prim sind, so wird durch diese als Elemente einer zweigliedrigen Basis eine Gruppe

$$(1) \qquad A^\alpha B^\beta \qquad \begin{array}{l} \alpha = 0, 1, 2 \ldots a-1 \\ \beta = 0, 1, 2 \ldots b-1 \end{array}$$

dargestellt. Dieselbe Gruppe kann aber auch durch die eingliedrige Basis AB dargestellt werden in der Form

$$(2) \qquad (AB)^s \qquad s = 0, 1, 2 \ldots ab-1.$$

Denn sind α und β beliebig gegeben, so kann man s nach dem Modul ab so bestimmen, dass

$$s \equiv \alpha \pmod{a}, \quad s \equiv \beta \pmod{b},$$

wodurch (2) mit (1) identisch wird. Trotzdem ist in gewissem Sinne die Constitution der Basis durch die Natur der Gruppen völlig bestimmt, nach dem folgenden Satze:

II. Sind

$$A_1, A_2 \ldots A_\nu$$

mit den Graden

$$a_1, a_2 \ldots a_\nu$$

und

$$B_1, B_2 \ldots B_\mu$$

mit den Graden

$$b_1, b_2 \ldots b_\mu$$

zwei Basen einer Abel'schen Gruppe S vom Grade n, ist p eine in n aufgehende Primzahl und

(1) $$a_1 = p_1 a'_1, \quad a_2 = p_2 a'_2, \ldots a_\nu = p_\nu a'_\nu,$$

(2) $$b_1 = p'_1 b'_1, \quad b_2 = p'_2 b'_2, \ldots b_\mu = p'_\mu b'_\mu,$$

worin $p_1, p_2 \ldots p_\nu, p'_1, p'_2 \ldots p'_\mu$ die höchsten Potenzen von p sind, die in $a_1, a_2 \ldots a_\nu, b_1, b_2 \ldots b_\mu$ aufgehen, so kommen alle Primzahlpotenzen $p_1, p_2 \ldots p_\nu$, die grösser als 1 sind, auch unter den $p'_1, p'_2 \ldots p'_\mu$ vor, und umgekehrt.

Um diesen Satz zu beweisen, nehmen wir die Elemente der beiden Basen A und B so geordnet an, dass

(3) $$\begin{aligned} p_1 &\geqq p_2 \geqq \cdots \geqq p_\nu \\ p'_1 &\geqq p'_2 \geqq \cdots \geqq p'_\mu. \end{aligned}$$

Die in (1) und (2) vorkommenden ganzen Zahlen $a'_1, a'_2 \ldots a'_\nu$, $b'_1, b'_2 \ldots b'_\mu$ sind nach ihrer Definition durch p nicht theilbar, und wenn wir also mit m das kleinste gemeinschaftliche Vielfache von $a'_1, a'_2 \ldots a'_\nu$ bezeichnen, so ist auch m nicht durch p theilbar. Ist aber

(4) $$\Theta = A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_\nu^{\alpha_\nu}$$

ein beliebiges Element von S, so folgt, dass

$$\Theta^{p_1 m} = 1$$

sein muss.

Setzt man hierin $B_1, B_2 \dots B_\mu$ für Θ, so folgt, dass $p_1 m$ durch jede der Zahlen $b_1, b_2 \dots b_\mu$ theilbar ist. Es ist also p_1 theilbar durch p'_1 und m durch das kleinste gemeinschaftliche Vielfache von $b'_1, b'_2 \dots b'_\mu$. In diesem Schlusse können wir nun durchweg A mit B vertauschen. Es muss also auch p'_1 durch p_1 theilbar sein, und daher

$$(5) \qquad p_1 = p'_1,$$

und ausserdem ergiebt sich, dass m auch das kleinste gemeinschaftliche Vielfache von $b'_1, b'_2 \dots b'_\mu$ ist.

Um daraus unseren Satz allgemein zu beweisen, nehmen wir an, es sei für irgend ein s bewiesen, dass

$$(6) \qquad p_1 = p'_1,\ p_2 = p'_2, \dots p_{s-1} = p'_{s-1}$$

sein müsse. Nach (4) ist für jedes Element Θ:

$$(7) \qquad \Theta^{p_s m} = A_1^{\alpha_1 p_s m} A_2^{\alpha_2 p_s m} \dots A_{s-1}^{\alpha_{s-1} p_s m},$$

worin m wie oben das kleinste gemeinschaftliche Vielfache von $a'_1, a'_2 \dots a'_\nu$ und zugleich von $b'_1, b'_2 \dots b'_\mu$, also durch p nicht theilbar ist.

Wir bestimmen nun die Anzahl der in der Form (7) enthaltenen von einander verschiedenen Elemente.

Lassen wir α_1 die Reihe der Zahlen $0, 1, 2 \dots \frac{p_1}{p_s} - 1$ durchlaufen, so sind die Elemente

$$(8) \qquad 1,\ A_1^{p_s m},\ A_1^{2 p_s m} \dots A_1^{\left(\frac{p_1}{p_s} - 1\right) p_s m}$$

alle von einander verschieden, während $A_1^{\frac{p_1}{p_s} p_s m}$ wieder $= 1$ wird, so dass sich alle anderen Potenzen $A_1^{\alpha_1 p_s m}$ in der Reihe (8) wiederfinden. Ebenso schliessen wir in Bezug auf die übrigen Factoren von (7), woraus man die genaue Anzahl der von einander verschiedenen in $\Theta^{p_s m}$ enthaltenen Elemente

$$(9) \qquad z = \frac{p_1}{p_s} \frac{p_2}{p_s} \dots \frac{p_{s-1}}{p_s}$$

findet.

Von den beiden Zahlen p_s, p'_s wird, wenn sie nicht gleich sind, eine die grössere sein. Wir wollen also annehmen, es sei

$$(10) \qquad p'_s \gtreqless p_s.$$

Nun drücken wir Θ durch die Basis B aus, und setzen

$$(11) \qquad \Theta^{p_s m} = B_1^{\beta_1 p_s m} B_2^{\beta_2 p_s m} \dots B_\mu^{\beta_\mu p_s m},$$

und wir zählen nun wieder ab, wie viel verschiedene Elemente in dieser Form enthalten sind. Die beiden Werthe für z müssen dann übereinstimmen.

Zählen wir, wie oben in (7), die Anzahl der verschiedenen in der Form

(12) $$B_1^{\beta_1 p_s m} B_2^{\beta_2 p_s m} \ldots B_{s-1}^{\beta_{s-1} p_s m}$$

enthaltenen Elemente, so ergiebt sich auch hierfür nach der Annahme (6) der Werth z. Es kann daher in der Form

(13) $$B_s^{\beta_s p_s m} \ldots B_\mu^{\beta_\mu p_s m}$$

nur das einzige Element 1 enthalten sein, woraus zu schliessen ist, dass p_s durch p'_s theilbar sein muss. Das ist aber mit (10) nur unter der Voraussetzung vereinbar, dass

(14) $$p_s = p'_s \text{ ist.}$$

Hiermit ist unser Theorem II. bewiesen.

Die in den Gradzahlen einer Basis von S enthaltenen Primzahlpotenzen sind also von der besonderen Wahl der Basis ganz unabhängig und wir nennen sie daher die **Invarianten der Gruppe**. Das Product aller Invarianten ist gleich dem Grade n der Gruppe.

Nach §. 9 können wir für S eine Basis bestimmen, bei der die Grade der Elemente lauter Primzahlpotenzen sind. Nach dem Theorem II. sind diese Grade die Invarianten der Gruppe und sind also durch die Gruppe vollständig bestimmt.

Dass die Invarianten auch die Natur der Gruppe vollständig bestimmen, ergiebt sich aus dem Satze:

III. **Zwei Gruppen mit denselben Invarianten sind isomorph, und isomorphe Gruppen haben dieselben Invarianten.**

Wenn nämlich zwei Gruppen S und S' der Anzahl und dem Grade nach übereinstimmende Basiselemente haben, wenn etwa

$$\Theta = A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_\nu^{\alpha_\nu}$$

die Elemente von S sind, und

$$\Theta' = B_1^{\alpha_1} B_2^{\alpha_2} \ldots B_\nu^{\alpha_\nu}$$

die Elemente von S', wo die $\alpha_1, \alpha_2 \ldots \alpha_\nu$ in beiden Fällen Restsysteme nach den Moduln $a_1, a_2 \ldots a_\nu$ durchlaufen, so brauchen wir nur Θ und Θ' dann einander entsprechen zu lassen, wenn

die Exponenten α in beiden dieselben sind; dann sind beide Gruppen isomorph auf einander bezogen.

Haben also zwei Gruppen dieselben Invarianten, so können wir diese Invarianten in beiden Gruppen zu Graden der Basiselemente machen, und erhalten dann diesen Fall.

Wenn umgekehrt zwei Gruppen isomorph sind, so bilden die den Basiselementen der einen Gruppe entsprechenden Elemente der anderen eine Basis der letzteren, und also müssen auch die Invarianten in beiden dieselben sein [1]).

§. 11.

Gruppencharaktere.

Es ist ein Hauptproblem in der Theorie der Abel'schen Gruppen, alle Theiler einer Abel'schen Gruppe zu finden. Die Lösung dieser Aufgabe wird wesentlich erleichtert durch die Einführung des Begriffes der Gruppencharaktere, der auch sonst in mancher Beziehung von Wichtigkeit ist.

Es sei S eine Abel'sche Gruppe n^{ten} Grades, deren Elemente durch A bezeichnet werden sollen, und es seien

$$(1) \qquad A_1, A_2 \ldots A_\nu$$

die Elemente einer Basis von S von den Graden $a_1, a_2 \ldots a_\nu$. Jedes Element A ist also, und zwar nur auf eine Weise, in der Form

$$(2) \qquad A = A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_\nu^{\alpha_\nu}$$

---

1) Ueber die Theorie der Abel'schen Gruppen ist zu vergleichen:

Gauss, Démonstration de quelques théorèmes concernant les périodes des classes des formes binaires du second degré. Werke, Bd. II, S. 266.

Schering, Die Fundamentalclassen der zusammensetzbaren arithmetischen Formen, Göttinger Abhandlungen, Bd. 14.

Frobenius und Stickelberger, Ueber Gruppen vertauschbarer Elemente. Crelle's Journal, Bd. 86, S. 217.

Weber, „Theorie der Abel'schen Zahlkörper", Acta mathematica, Bd. 8 u. 9.

Der Begriff der Invarianten ist zuerst eingeführt in der Abhandlung von Frobenius und Stickelberger, aber etwas anders definirt als hier. Dieser älteren Definition, die sich bei der Anwendung auf die Kreistheilungszahlen minder zweckmässig erweist, ist der Verfasser in der citirten Abhandlung in den Acta mathematica gefolgt.

darstellbar, so dass

(3) $$0 \leqq \alpha_1 < a_1,\ 0 \leqq \alpha_2 < a_2, \ldots 0 \leqq \alpha_\nu < a_\nu.$$

Die Exponenten $\alpha_1, \alpha_2 \ldots \alpha_\nu$ oder irgend welche ihnen nach den Moduln $a_1, a_2 \ldots a_\nu$ congruente Zahlen heissen die **Indices** des Elementes A, und es gilt der Satz:

1. Man erhält die Indices eines Compositums AA', wenn man die entsprechenden Indices der beiden Factoren addirt.

Wenn wir jedem Elemente A irgendwie einen **Zahlenwerth** zuordnen, so können wir diese Zuordnung eine **Function** von A nennen. Eine solche Function $\chi(A)$ soll nun ein **Gruppencharakter** genannt werden, wenn sie für je zwei Elemente A, A' von S der Bedingung genügt:

(4) $$\chi(AA') = \chi(A)\chi(A'),$$

und folglich auch der allgemeineren

$$\chi(A\,A'\,A'' \ldots) = \chi(A)\,\chi(A')\,\chi(A'') \ldots$$

Zwei solche Functionen χ und χ_1 werden als verschieden angesehen, wenn es wenigstens ein Element A giebt, wofür $\chi(A)$ von $\chi_1(A)$ verschieden ist. Diese Charaktere wollen wir nun näher bestimmen.

Setzen wir $A' = 1$, so ergiebt sich aus (4):

(5) $$\chi(A) = \chi(A)\chi(1),$$

und wenn wir ein für allemal den Fall ausschliessen, dass alle $\chi(A) = 0$ sind:

(6) $$\chi(1) = 1,$$

also der erste Satz:

2. Jeder Charakter hat für das Einheitselement den Werth 1.

Setzen wir ferner $A' = A$, so folgt aus (4):

$$\chi(A^2) = [\chi(A)]^2,$$

und daraus durch vollständige Induction für jeden Exponenten h:

(7) $$\chi(A^h) = \chi(A)^h.$$

Bezeichnen wir also mit a den Grad des Elementes A, so folgt, wenn man in (7) $h = a$ setzt und (6) benutzt:

(8) $$\chi(A)^a = 1,$$

also:

3. **Die Werthe eines Charakters $\chi(A)$ sind Einheitswurzeln, deren Grad ein Theiler des Grades von A ist.**

Danach können wir leicht alle Charaktere bestimmen. Setzen wir nämlich

(9) $$\chi(A_1) = \omega_1,\ \chi(A_2) = \omega_2 \ldots \chi(A_\nu) = \omega_\nu,$$

so ist

(10) $$\omega_1^{a_1} = 1,\ \omega_2^{a_2} = 1, \ldots \omega_\nu^{a_\nu} = 1,$$

und es ist nach (2) und (4)

(11) $$\chi(A) = \omega_1^{\alpha_1}\omega_2^{\alpha_2} \ldots \omega_\nu^{\alpha_\nu}.$$

Umgekehrt ist, wenn $\omega_1, \omega_2 \ldots \omega_\nu$ irgend eine Lösung der Gleichungen (10) bedeutet, durch (11) eine Function von A bestimmt, die nach 1. der Bedingung (4) genügt und also ein Charakter der Gruppe ist.

Jede der Gleichungen (10) hat $a_1, a_2 \ldots a_\nu$ Wurzeln, und wenn wir jede mit jeder combiniren, so ergeben sich

$$a_1 a_2 \ldots a_\nu = n$$

Combinationen. Alle diese Combinationen führen zu verschiedenen Charakteren $\chi(A)$. Denn bezeichnen wir mit $\omega_1', \omega_2' \ldots \omega_\nu'$ eine zweite Combination von Wurzeln der Gleichung (10), und ist für alle Elemente A

$$\omega_1^{\alpha_1}\omega_2^{\alpha_2} \ldots \omega_\nu^{\alpha_\nu} = \omega_1'^{\alpha_1}\omega_2'^{\alpha_2} \ldots \omega_\nu'^{\alpha_\nu},$$

so folgt, wenn man $\alpha_1 = 1,\ \alpha_2 = 0 \ldots \alpha_\nu = 0$ setzt, $\omega_1 = \omega_1'$ und ebenso $\omega_2 = \omega_2' \ldots \omega_\nu = \omega_\nu'$. Daraus folgt der Satz:

4. **Es giebt n und nicht mehr verschiedene Charaktere einer Abel'schen Gruppe n^{ten} Grades, die alle durch die Formel (11) dargestellt sind.**

Wenn wir unter $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_\nu$ ein System **primitiver Wurzeln** der Gleichungen (10) verstehen, so können wir

(12) $$\omega_1 = \varepsilon_1^{\beta_1},\ \omega_2 = \varepsilon_2^{\beta_2}, \ldots \omega_\nu = \varepsilon_\nu^{\beta_\nu}$$

setzen, und können die $\beta_1, \beta_2 \ldots \beta_\nu$ ebenso wie die $\alpha_1, \alpha_2 \ldots \alpha_\nu$ je einem vollen Restsysteme nach den Moduln $a_1, a_2 \ldots a_\nu$ entnehmen. Dann bekommen wir die sämmtlichen n Gruppencharaktere bei feststehenden $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_\nu$ in der Form

(13) $$\chi(A) = \varepsilon_1^{\alpha_1\beta_1}\varepsilon_2^{\alpha_2\beta_2} \ldots \varepsilon_\nu^{\alpha_\nu\beta_\nu}.$$

Unter diesen Charakteren kommt auch der vor, den man erhält, wenn man $\beta_1 = 0$, $\beta_2 = 0 \ldots \beta_\nu = 0$ setzt, der für alle Elemente A den Werth 1 hat. Diesen wollen wir den **Einheitscharakter** nennen.

Die n Charaktere von S können nun selbst wieder zu einer Abel'schen Gruppe vereinigt werden, und zwar zu einer mit S isomorphen Gruppe.

Nach (13) ist nämlich jeder der n Charaktere durch ein nach dem Modulsysteme $a_1, a_2 \ldots a_\nu$ genommenes Zahlensystem $\beta_1, \beta_2 \ldots \beta_\nu$ bestimmt, und dies Zahlensystem der β ist zugleich das System der Indices eines bestimmten Elementes B von S, nämlich von

(14) $$B = A_1^{\beta_1} A_2^{\beta_2} \ldots A_\nu^{\beta_\nu},$$

so dass jedem Elemente B von S ein bestimmter Charakter entspricht, den wir mit $\chi_B(A)$ oder, indem wir A weglassen, mit χ_B bezeichnen. Diese Zuordnung der Charaktere χ zu den Elementen B wird sich aber ändern, wenn eine andere Basis zu Grunde gelegt wird, oder wenn die Einheitswurzeln $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_\nu$ anders angenommen werden.

Ist B' ein zweites Element von S mit den Indices $\beta'_1, \beta'_2 \ldots \beta'_\nu$, so erhalten wir in gleicher Weise den Charakter $\chi_{B'}$, und wenn wir nun unter $\chi_{BB'}$ den Charakter verstehen, der für jedes A durch die Formel

(15) $$\chi_{BB'}(A) = \varepsilon_1^{\alpha_1(\beta_1 + \beta_1')} \varepsilon_2^{\alpha_2(\beta_2 + \beta_2')} \ldots \varepsilon_\nu^{\alpha_\nu(\beta_\nu + \beta_\nu')}$$

bestimmt ist, so sind die Charaktere χ hierdurch zu einer mit S isomorphen Gruppe verbunden. Das Einheitselement in dieser **Charakterengruppe** ist der Einheitscharakter.

Es lässt sich hiernach auch die Gruppe der Charaktere durch eine Basis darstellen, die man erhält, wenn man

(16) $$\chi_1(A) = \varepsilon_1^{\alpha_1}, \; \chi_2(A) = \varepsilon_2^{\alpha_2} \ldots \chi_\nu(A) = \varepsilon_\nu^{\alpha_\nu}$$

setzt. Dann ist jeder Charakter in der Form enthalten:

(17) $$\chi_B = \chi_1^{\beta_1} \chi_2^{\beta_2} \ldots \chi_\nu^{\beta_\nu},$$

und es ist, wenn B, B' zwei Elemente in S sind:

(18) $$\chi_B \chi_{B'} = \chi_{BB'}.$$

Sind χ_1, χ_2 irgend zwei der Charaktere und $\chi_1 \chi_2$ der aus beiden zusammengesetzte, so ist nach (15) für jedes Element A

(19) $$\chi_1(A)\, \chi_2(A) = \chi_1 \chi_2(A).$$

Wir wollen das gewonnene Resultat noch als Satz aussprechen:

5. Die Charaktere einer Gruppe S können zu einer mit S isomorphen Gruppe verbunden werden.

Es sei noch der Satz erwähnt, der sich aus der Definition von χ_B durch die Formel (13) unmittelbar ergiebt:

$$\chi_B(A) = \chi_A(B). \tag{20}$$

Endlich gilt auch noch der folgende Satz:

6. Durchläuft A alle Elemente der Gruppe S, so ist für einen feststehenden Charakter χ:

$$\sum^{A} \chi(A) = n \text{ oder } = 0, \tag{21}$$

je nachdem χ der Einheitscharakter ist oder nicht. Ebenso ist, wenn das Element A festgehalten wird und χ die Reihe der Charaktere durchläuft:

$$\sum^{\chi} \chi(A) = n \text{ oder } = 0, \tag{22}$$

je nachdem A das Einheitselement ist oder nicht.

Für den Fall, dass χ oder A die Einheitselemente ihrer Gruppen sind, sind die Formeln (21) und (22) evident, da dann jedes der n Glieder der Summe den Werth 1 hat. Ist aber χ nicht der Einheitscharakter, so giebt es ein Element B in S, so dass $\chi(B)$ nicht $= 1$ ist. Setzen wir dann

$$\sum^{A} \chi(A) = \sigma,$$

so folgt durch Multiplication mit $\chi(B)$:

$$\sum^{A} \chi(AB) = \sigma \chi(B).$$

Da aber AB zugleich mit A die ganze Gruppe S durchläuft, so ist auch $\sum^{A} \chi(AB) = \sigma$, also $\sigma[1 - \chi(B)] = 0$ oder $\sigma = 0$, w. z. b. w.

Ebenso beweist man die Formel (22), die übrigens auch nach (20) unmittelbar aus (21) folgt.

§. 12.

Divisoren einer Abel'schen Gruppe. Reciproke Gruppen.

Ein Theiler T einer Abel'schen Gruppe S ist, wie schon oben bemerkt, immer ein Normaltheiler, und daher giebt es nach §. 4 eine zu T complementäre Gruppe

$$S/T,$$

deren Elemente die Nebengruppen von T sind, nämlich

(1) $$T,\ TA',\ TA'' \ldots,$$

worin $A', A'' \ldots$ gewisse Elemente aus S bedeuten. Die Anzahl der Elemente (1), also der Grad der Gruppe S/T ist, wenn t der Grad von T ist, gleich dem Index des Theilers T von S, also gleich

$$\frac{n}{t} = j.$$

Diese Gruppe S/T ist aber selbst wieder eine Abel'sche; denn es ist

$$TA'\,TA'' = TA'A'',\quad TA''\,TA' = TA''A',$$

also beides einander gleich.

Es sind nun die Charaktere der Gruppe S/T zu bestimmen. Wir bezeichnen die Elemente dieser Gruppe mit

(2) $$T,\ T_1,\ T_2 \ldots T_{j-1},$$

und einen ihrer Charaktere mit $\xi(T_i)$.

Aus dieser Function $\xi(T)$ können wir nun eine Function $\xi(A)$ der Elemente von S ableiten, indem wir

(3) $$\xi(A_i) = \xi(T_i)$$

setzen, wenn A_i irgend ein in der Nebengruppe T_i vorkommendes Element ist. Für die Elemente der Gruppe T selbst ist dann $\xi(A) = 1$.

Diese Function $\xi(A_i)$ ist aber unter den Charakteren von S enthalten. Denn wenn A_i in T_i und A_k in T_k vorkommt, so kommt $A_i A_k$ in $T_i T_k$ vor, und folglich ist

(4) $$\xi(A_i)\,\xi(A_k) = \xi(T_i)\,\xi(T_k) = \xi(T_i T_k) = \xi(A_i A_k).$$

Dies aber ist nach §. 11, (4) die Definition für einen Charakter von S.

Wenn umgekehrt einer der Charaktere $\chi = \xi$ der Gruppe S für alle Elemente der Gruppe T denselben Werth hat, so kann dies nur der Werth 1 sein, da in T sicher das Einheitselement von S vorkommt (§. 11, 2.). Wenn dann A_i irgend ein Element aus T_i ist, und A die ganze Gruppe T durchläuft, so durchläuft $A A_i$ die Nebengruppe T_i. Es ist dann aber $\xi(A) = 1$ und folglich

$$\xi(A A_i) = \xi(A_i), \tag{5}$$

d. h. $\xi(A)$ hat für alle Elemente einer Nebengruppe T_i einen und denselben Werth, und $\xi(A)$ kann also als Function von T_i aufgefasst und mit $\xi(T_i)$ bezeichnet werden.

Da nun, wenn A_i in T_i und A_k in T_k vorkommt, $A_i A_k$ in $T_i T_k$ enthalten ist, so folgt

$$\xi(T_i)\,\xi(T_k) = \xi(T_i T_k), \tag{6}$$

d. h. $\xi(T_i)$ ist unter den Charakteren der Gruppe S/T enthalten. Es giebt also genau j solche Charaktere $\xi(A)$, die dadurch definirt sind, dass sie für jedes Element in T den Werth 1 haben. Diese j Charaktere ξ bilden nach der Composition der Charaktere eine Gruppe; denn ist $\xi_1(A) = 1$, $\xi_2(A) = 1$, so ist auch $\xi_1 \xi_2(A) = 1$ [§. 11, (18)]. Da die Functionen ξ nach (4) auch als die Charaktere der Gruppe S/T aufgefasst werden können, so ist nach §. 11, 5. die Gruppe der ξ mit der Gruppe S/T isomorph.

Damit ist also der folgende Satz bewiesen:

7. Hat eine Abel'sche Gruppe S einen Theiler T vom Grade t und vom Index j, so giebt es unter den Charakteren von S genau j und nicht mehr, die für alle Elemente von T den Werth 1 haben, während für jedes nicht in T enthaltene Element von S wenigstens einer von ihnen von 1 verschieden ist. Diese Charaktere bilden eine mit S/T isomorphe Gruppe.

Wir wollen diese Charaktere zur Gruppe T gehörig nennen.

Da jeder Charakter χ_B einem bestimmten Elemente B von S entspricht, so wird auch, wenn χ_B die Gruppe der zu T gehörigen Charaktere durchläuft, B wegen der Formel §. 11, (18) eine Gruppe durchlaufen, die vom Grade j und mit der Gruppe der χ_B und also auch mit der Gruppe S/T isomorph ist. Diese

Gruppe der B, die also auch ein Theiler von S ist, wollen wir mit U bezeichnen und die zu T reciproke Gruppe nennen. Auch hier ist aber zu bemerken, dass der Begriff der reciproken Gruppe im Allgemeinen von der Wahl der Basis und der Einheitswurzeln ε abhängt, also nicht zu den Gruppen S und T als solchen gehört.

Die zu T reciproke Gruppe ist durch folgenden Satz charakterisirt:

8. Lässt man A die Elemente eines Theilers T von S durchlaufen und sucht alle Elemente B von S, die für jedes A der Bedingung

$$\chi_B(A) = 1 \tag{7}$$

genügen, so durchläuft B die Elemente der zu T reciproken Gruppe U, deren Grad gleich dem Index von T ist.

Nach dem Satze §. 11, (20) ist T die reciproke Gruppe zu U, die Beziehung dieser beiden Gruppen also eine gegenseitige.

Von diesen reciproken Gruppen gilt noch der Satz:

9. Ist T' ein Theiler von T, so ist umgekehrt die reciproke Gruppe U von T ein Theiler der zu T' reciproken Gruppe U'.

Denn jedes Element A' von T' ist zugleich in T enthalten, und folglich ist, wenn B die Gruppe U durchläuft, $\chi_B(A') = 1$. Es muss also B in der Gruppe U' vorkommen.

Wählt man aus der Gesammtheit der Charaktere χ eine beliebige Anzahl $\xi_1, \xi_2 \ldots \xi_\mu$ aus, gleichviel ob sie eine Gruppe bilden oder nicht, so bilden alle Elemente A, die den μ Bedingungen

$$\xi_1(A) = 1,\ \xi_2(A) = 1, \ldots \xi_\mu(A) = 1 \tag{8}$$

genügen, eine Gruppe, weil aus $\xi_i(A) = 1$, $\xi_i(A') = 1$ folgt, dass auch $\xi_i(AA') = 1$ ist. Wenn die $\xi_1, \xi_2 \ldots \xi_\mu$ keine Gruppen sind, so folgen aus den Gleichungen (8) noch so viele weitere $\xi_{\mu+1}(A) = 1 \ldots$, dass die $\xi_1, \xi_2 \ldots \xi_\mu$ zu einer Gruppe ergänzt werden.

10. Aus dem Theorem 7. folgt, dass man so alle möglichen Theiler von S erhalten kann.

Es ist vielleicht erwünscht, diese Sätze an einem einfachen Beispiele zu erläutern. Es sei der Grad der Gruppe S das Quadrat einer Primzahl $n = p^2$. Dann hat S entweder nur die eine Invariante p^2 und ist dann cyklisch:

a) $$S = 1, A, A^2 \dots A^{p^2-1},$$

oder es hat S zwei Invarianten, die beide gleich p sind; dann besteht S aus den Elementen:

b) $$S = A_1^{\alpha_1} A_2^{\alpha_2}, \quad \alpha_1, \alpha_2 = 0, 1 \dots p-1.$$

Im Falle a) erhalten wir die p^2 Charaktere

$$\chi_B(A^\alpha) = \varepsilon^{\beta\alpha},$$

wenn ε eine primitive Wurzel der Gleichung $\varepsilon^{pp} = 1$ ist. Nehmen wir, um nach dem Satze 10. die Theiler von S zu bilden, einen der Charaktere χ_B, in dem β nicht durch p theilbar ist, so wird $\chi_B(A^\alpha)$ nur dann $= 1$ sein können, wenn α durch p^2 theilbar oder also $= 0$ ist, d. h. wir bekommen nur den aus dem Einheitselemente bestehenden Theiler von S. Nehmen wir aber $\beta = p\beta'$ durch p, aber nicht durch p^2 theilbar an, so wird $\chi_{p\beta'}(A^\alpha)$ dann und nur dann $= 1$, wenn $\alpha = p\alpha'$ durch p theilbar ist. Wir erhalten also den Theiler

$$T = 1, A^p, A^{2p} \dots A^{(p-1)p},$$

und der zu T reciproke Theiler U ist hier mit T identisch.

Im Falle b) müssen wir, um die Charaktere zu bilden, zwei p^{te} Einheitswurzeln $\varepsilon^{\beta_1}, \varepsilon^{\beta_2}$ annehmen, und erhalten, wenn

$$B = A_1^{\beta_1} A_2^{\beta_2}$$

gesetzt ist,

$$\chi_B(A_1^{\alpha_1} A_2^{\alpha_2}) = \varepsilon^{\alpha_1\beta_1 + \alpha_2\beta_2}.$$

Setzen wir zwei dieser Charaktere $= 1$, also

$$\alpha_1\beta_1 + \alpha_2\beta_2 \equiv 0, \quad \alpha_1\beta_1' + \alpha_2\beta_2' \equiv 0,$$

so folgt, wenn die Determinante $\beta_1\beta_2' - \beta_2\beta_1'$ nicht durch p theilbar ist, dass α_1 und α_2 durch p theilbar sein müssen. Ist aber die Determinante durch p theilbar, so ist die eine dieser beiden Congruenzen eine Folge der anderen. Im ersten Falle bekommen wir also eine Gruppe, die nur aus dem Einheitselemente besteht. Wir erhalten daher alle von 1 und S verschiedenen Theiler T_{β_1,β_2}, wenn wir für ein feststehendes β_1, β_2 die α_1, α_2 auf alle möglichen Arten der Congruenz

(9) $$\alpha_1\beta_1 + \alpha_2\beta_2 \equiv 0 \pmod{p}$$

gemäss bestimmen. Ist α_1, α_2 eine Lösung dieser Congruenz, in der nicht beide Zahlen Null sind, so erhalten wir alle Lösungen, wenn wir in $h\alpha_1, h\alpha_2$ den Factor h die Reihe der Zahlen $0, 1 \ldots p-1$ durchlaufen lassen, und die Gruppe T wird also, wenn α_1, α_2 ein festes, der Bedingung (9) genügendes Werthpaar ist,

$$(A_1^{\alpha_1} A_2^{\alpha_2})^h, \qquad h = 0, 1, \ldots p-1.$$

Die reciproke Gruppe U erhält man, wenn man alle Werthe der β sucht, die der Bedingung (9) genügen, und man findet also die Gruppe U in der Form

$$(A_1^{\beta_1} A_2^{\beta_2})^h, \qquad h = 0, 1, \ldots p-1,$$

worin $\alpha_1, \alpha_2, \beta_1, \beta_2$ jetzt vier feste, der Bedingung (9) genügende Zahlen sind. Setzt man $\beta_1 = 0$, $\beta_2 = 1$, $\alpha_1 = 1$, $\alpha_2 = 0$, so erhält man den besonderen Fall der beiden reciproken Gruppen

$$A_1^h, A_2^h, \qquad h = 0, 1, \ldots p-1.$$

§. 13.

Die Geschlechter in einer Abel'schen Gruppe.

Ein Element einer Abel'schen Gruppe S, das mit seinem entgegengesetzten identisch ist, dessen zweite Potenz also gleich dem Einheitselemente ist, wird ein zweiseitiges Element [1]) genannt. Das Einheitselement gehört also immer zu den zweiseitigen.

Stellen wir die Elemente von S durch eine Basis $A_1, A_2 \ldots A_\nu$ dar, deren Elemente die Grade $a_1, a_2 \ldots a_\nu$ haben, so wird

$$(1) \qquad A = A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_\nu^{\alpha_\nu}$$

dann und nur dann ein zweiseitiges Element sein, wenn

$$(2) \qquad 2\alpha_1 \equiv 0 \pmod{a_1},\ 2\alpha_2 \equiv 0 \pmod{a_2}, \ldots 2\alpha_\nu \equiv 0 \pmod{a_\nu}.$$

Wenn nun unter den Invarianten der Gruppe λ mal eine Potenz von 2 vorkommt, so können wir die Basis von S so geordnet annehmen, dass $a_1, a_2 \ldots a_\lambda$ gerade, $a_{\lambda+1} \ldots a_\nu$ ungerade Zahlen sind. Dann ergeben sich die Lösungen von (2):

[1]) Vergl. Bd. I, S. 390, Anmerkung.

$$\alpha_1 = \frac{\eta_1 a_1}{2}, \alpha_2 = \frac{\eta_2 a_2}{2} \dots \alpha_\lambda = \frac{\eta_\lambda a_\lambda}{2}, \alpha_{\lambda+1} = 0 \dots \alpha_\nu = 0,$$

worin $\eta_1, \eta_2 \dots \eta_\lambda$ gleich 0 oder gleich 1 sein können, und man erhält alle zweiseitigen Elemente in der Form

$$A_1^{\frac{\eta_1 a_1}{2}} A_2^{\frac{\eta_2 a_2}{2}} \dots A_\lambda^{\frac{\eta_\lambda a_\lambda}{2}},$$

und ihre Anzahl ist, da alle Combinationen von 0 und 1 für die Exponenten η zulässig sind, $= 2^\lambda$.

Ist χ ein beliebiger Charakter von S, so ist, wenn A ein zweiseitiges Element ist, $\chi(A) = \pm 1$, da

$$\chi(A)^2 = \chi(1) = 1$$

ist.

Ebenso nennen wir einen zweiseitigen Charakter einen solchen, der in der Gruppe der Charaktere ein zweiseitiges Element ist. Da die Gruppe der Charaktere mit der Gruppe S isomorph ist, so giebt es ebenso viele zweiseitige Charaktere als zweiseitige Elemente, nämlich 2^λ. Sie werden nach §. 11, (17) dargestellt durch:

$$\chi_1^{\frac{\eta_1 a_1}{2}} \chi_2^{\frac{\eta_2 a_2}{2}} \dots \chi_\lambda^{\frac{\eta_\lambda a_\lambda}{2}}.$$

Die zweiseitigen Charaktere haben für jedes Element den Werth ± 1.

Die zweiseitigen Elemente bilden für sich eine Gruppe T vom Grade 2^λ. Ebenso bilden die zweiseitigen Charaktere eine damit isomorphe Gruppe, und man erhält die zu T reciproke Gruppe U, wenn man alle Elemente A aufsucht, für die alle zweiseitigen Charaktere den Werth $+1$ haben. Diese Gruppe, die nach §. 12, 7. ein Theiler von S vom Index 2^λ ist, ist nach der letzten Definition weder von der Wahl der Basis noch von den die Charaktere darstellenden Einheitswurzeln abhängig, und ist durch die Natur der Gruppe S vollständig bestimmt. Bezeichnen wir sie mit G, so ist das System der Nebengruppen

(3) $$G, G_1, G_2 \dots G_{2^\lambda - 1}$$

dadurch charakterisirt, dass für alle Elemente eines dieser Systeme die zweiseitigen Charaktere ein und dasselbe Werthsystem ergeben. Die Systeme $G, G_1, G_2 \dots$ werden die in S enthaltenen Geschlechter (Genera) genannt. Die Gruppe G speciell heisst das Hauptgeschlecht.

Die Anzahl der Geschlechter ist also so gross, wie die Anzahl der zweiseitigen Elemente[1]).

§. 14.

Indices nach einer ungeraden Primzahlpotenz als Modul.

Das wichtigste Beispiel einer commutativen Gruppe bieten die natürlichen Zahlen, wenn sie durch die gewöhnliche Multiplication mit einander verbunden werden.

Um daraus eine endliche Gruppe abzuleiten, nehmen wir eine beliebige ganze positive Zahl m als Modul an und zerlegen m in seine Primfactoren

(1) $$m = 2^{\lambda} q_1^{\varkappa_1} q_2^{\varkappa_2} \ldots,$$

worin $q_1, q_2 \ldots$ verschiedene ungerade Primzahlen, $\lambda, \varkappa_1, \varkappa_2 \ldots$ positive Exponenten, λ möglicherweise auch die Null, nämlich wenn m ungerade ist, bedeuten.

Nun werden alle Zahlen, positive sowohl als negative, die nach dem Modul m unter einander congruent sind, in eine Zahlclasse vereinigt, und jede dieser Zahlclassen wird durch einen Repräsentanten, etwa durch den Rest der Division, also durch eine der Zahlen $0, 1, 2 \ldots m - 1$, dargestellt.

Sind a und a' zwei Zahlen einer solchen Classe und b und b' zwei Zahlen einer zweiten Classe, so gehören auch die Producte ab und $a'b'$ in dieselbe Classe. Denn ist $a \equiv a'$, $b \equiv b'$, so ist auch $ab \equiv a'b'$ (mod m). Durch die Multiplication werden also nicht bloss die Zahlen, sondern auch die Classen componirt.

Trotzdem bilden diese Zahlclassen in ihrer Gesammtheit noch keine Gruppe; denn aus einer Congruenz

$$ab \equiv ac \pmod{m}$$

folgt nur dann nothwendig $b \equiv c$, wenn a relativ prim zu m ist. Es ist also die Forderung §. 1, 3. hier im Allgemeinen nicht erfüllt.

Der grösste gemeinschaftliche Theiler, den eine Zahl a mit m hat, ist bei der ganzen durch a repräsentirten Classe der-

---

[1]) Gauss hat in die Theorie der quadratischen Formen diese Begriffe zuerst eingeführt, und den Ausdruck „Genera" gebraucht. Disqu. arithm. art. 228 f.

selbe, und kann der Theiler der Classe genannt werden. Sind d, d' die Theiler zweier Classen a, a', so ist der grösste gemeinschaftliche Theiler von m und dd' der Theiler der Classe aa'. Daraus ergiebt sich, dass die Zahlclassen, deren Zahlen relativ prim zu m sind, durch Composition immer wieder solche Zahlclassen ergeben, und für diese ist dann auch die Forderung §. 1, 3. erfüllt.

1. Die Zahlclassen, deren Individuen relativ prim zum Modul sind, bilden also bei der Composition durch Multiplication eine Abel'sche Gruppe.

Diese Gruppe ist der Gegenstand unserer Betrachtungen, wobei unser Hauptziel die Bestimmung einer Basis sein soll.

Wir wollen jede Zahlclasse, die nur zu m theilerfremde Zahlen enthält, mit N bezeichnen, und die Gruppe der Zahlclassen N, deren Existenz wir jetzt nachgewiesen haben, mit $\mathfrak{N}$. Mit n wollen wir jede zu m theilerfremde Zahl bezeichnen.

Der Grad dieser Gruppe ist so gross, wie die Anzahl der relativen Primzahlen zu m, die zugleich positiv und nicht grösser als m sind, und diese Zahl haben wir in §. 132 des ersten Bandes bestimmt. Sie ist

(2) $$\mu = \varphi(m) = 2^{\lambda-1}\, q_1^{\varkappa_1-1}(q_1-1)\, q_2^{\varkappa_2-1}(q_2-1)\ldots$$

oder

$$= q_1^{\varkappa_1-1}(q_1-1)\, q_2^{\varkappa_2-1}(q_2-1)\ldots,$$

wenn $\lambda = 0$ ist.

Der Grad eines Elementes N dieser Gruppe ist der kleinste positive Exponent e, zu dem man einen Repräsentanten n von N erheben muss, damit n^e der Einheit congruent wird nach dem Modul m. Da jedes e ein Theiler des Grades der Gruppe $\varphi(m)$ sein muss, so folgt der verallgemeinerte Fermat'sche Lehrsatz:

(3) $$n^{\varphi(m)} \equiv 1 \pmod{m},$$

eine Formel, die für jede zu m theilerfremde Zahl n gilt.

Ist nun q einer der ungeraden Primfactoren von m, und $q^\varkappa$ die höchste in m aufgehende Potenz von q, so nehmen wir eine primitive Wurzel g von q an, die wir, wenn $\varkappa$ grösser als 1 ist, so wählen, dass $g^q - g$ nicht durch q^2 theilbar ist (Bd. I, §. 184). Der Kürze wegen wollen wir eine dieser letzten Bedingung genügende Zahl g eine primitive Wurzel von q^2 nennen.

Ist nun $\varkappa = 1$, so sind nach der Definition von g die Zahlen

$$1, g, g^2 \ldots g^{q-2}$$

nach dem Modul q alle von einander verschieden, während g^{q-1} wieder congruent mit 1 ist.

Ist aber $\varkappa > 1$, so ist:

$$g^{q-1} = 1 + hq, \tag{4}$$

und nach unserer Voraussetzung über g ist h nicht durch q theilbar. Wenn wir die Gleichung (4) in die Potenz q erheben, und rechts den binomischen Lehrsatz anwenden, so ergiebt sich

$$g^{q(q-1)} = 1 + hq^2 + h^2 \frac{q^3(q-1)}{2} + \cdots,$$

also

$$g^{q(q-1)} = 1 + h_1 q^2, \tag{5}$$

worin

$$h_1 = h + h^2 \frac{q(q-1)}{2} + \cdots$$

nicht durch q theilbar ist. (Das wäre für $q = 2$ nicht mehr richtig und darum verlangt die Primzahl 2 eine andere Behandlung.)

Erheben wir (5) nochmals in die q^{te} Potenz, so ergiebt sich

$$g^{q^2(q-1)} = 1 + h_2 q^3,$$

und so können wir fortfahren und erhalten für jeden beliebigen positiven Exponenten λ

$$g^{q^{\lambda-1}(q-1)} = 1 + hq^{\lambda}, \tag{6}$$

worin h eine durch q nicht theilbare ganze Zahl ist. Setzen wir zur Abkürzung:

$$q^{\varkappa-1}(q-1) = \varphi(q^{\varkappa}) = c, \tag{7}$$

so ist also

$$g^c \equiv 1 \pmod{q^{\varkappa}}, \tag{8}$$

und es ist noch nachzuweisen, dass c der kleinste positive Exponent ist, für den die Congruenz (8) erfüllt ist. Nehmen wir an, es sei e dieser kleinste Exponent, also

$$g^e \equiv 1 \pmod{q^{\varkappa}}, \tag{9}$$

so muss e ein Theiler von c sein, weil sonst die Congruenz (8) auch erfüllt wäre, wenn c durch den Rest der Division von c durch e, der kleiner als e ist, ersetzt wird.

Andererseits muss e durch $q - 1$ theilbar sein, weil die in (9) enthaltene Congruenz $g^e \equiv 1 \pmod{q}$ nur für solche Exponenten, die durch $q - 1$ theilbar sind, besteht.

Es ist also e von der Form $q^{\lambda-1}(q-1)$ mit einem positiven λ. Dass aber λ nicht kleiner als $\varkappa$ sein kann, folgt aus (6), woraus zu sehen ist, dass q^λ die höchste Potenz von q ist, die in der Differenz

$$g^{q^{\lambda-1}(q-1)} - 1$$

aufgeht. Es ist also c die kleinste positive Zahl, für die die Congruenz (8) erfüllt ist, und damit ist gleichbedeutend, dass die Zahlen

(10) $$1, g, g^2 \ldots g^{c-1}$$

alle incongruent sind nach dem Modul $q^\varkappa$; g kann also auch als primitive Wurzel von $q^\varkappa$ bezeichnet werden.

Die Anzahl der Glieder dieser Reihe (10) ist gleich c. Ebenso gross ist aber auch die Anzahl der nach dem Modul $q^\varkappa$ incongruenten, durch q nicht theilbaren Zahlen n, und damit ist bewiesen:

2. Wenn q eine ungerade Primzahl, n eine beliebige durch q nicht theilbare Zahl, g eine primitive Wurzel von q^2 und $\varkappa$ ein positiver Exponent ist, so lässt sich eine und nur eine Zahl γ nach dem Modul c bestimmen, die der Congruenz

$$n \equiv g^\gamma \pmod{q^\varkappa}$$

genügt.

Die Zahl c ist immer durch 2 theilbar, und wir heben also noch den besonderen Satz hervor, dass

(11) $$g^{\frac{1}{2}c} \equiv -1 \pmod{q^\varkappa}$$

ist. Denn in dem durch $q^\varkappa$ theilbaren Producte

$$g^c - 1 = (g^{\frac{1}{2}c} - 1)(g^{\frac{1}{2}c} + 1)$$

ist der erste Factor nicht durch $q^\varkappa$ theilbar, und folglich muss der zweite Factor durch q theilbar sein. Dann folgt aber, dass der erste Factor auch nicht durch q theilbar sein kann, weil sonst auch die Summe der beiden Factoren, also auch g selbst, durch q theilbar sein müsste. Folglich muss der zweite Factor durch $q^\varkappa$ theilbar sein.

Hier besteht also vollständige Analogie mit den Sätzen über primitive Wurzeln und Indexsysteme, die wir im §. 136 des ersten Bandes kennen gelernt haben, und man kann also auch hier γ als den Index von n für den Modul $q^\varkappa$ bezeichnen.

§. 15.

Indices für eine Potenz von 2 als Modul.

Ein ähnlicher Satz muss nun für die Potenzen 2^λ der Primzahl 2 aufgestellt werden, die sich, wie schon vorhin bemerkt, anders verhält.

Ist $\lambda = 1$, so ist jede durch 2 nicht theilbare Zahl $n \equiv 1 \pmod 2$. Ist $\lambda = 2$, so ist -1 als primitive Wurzel von 4 aufzufassen, denn jede ungerade Zahl n genügt einer der Congruenzen

$$n \equiv (-1)^\alpha \pmod 4,$$

worin $\alpha = 0$ oder $= 1$ ist.

Aber schon für den Modul 8 existirt keine primitive Wurzel mehr, d. h. keine Zahl, durch deren Potenzen sich alle Zahlclassen ungerader Zahlen nach dem Modul 8 darstellen lassen. Denn ist g irgend eine ungerade Zahl, so sind unter den Potenzen von g höchstens die beiden $1, g$ nach dem Modul 8 verschieden, weil immer $g^2 \equiv 1 \pmod 8$ ist. Nimmt man also g nicht congruent 1 und nicht congruent $-1 \pmod 8$, also $g = 3$ oder $= 5$, so ist jede ungerade Zahl einer der vier Zahlen

$$(-1)^\alpha g^\beta \quad \alpha = 0, 1, \quad \beta = 0, 1$$

nach dem Modul 8 congruent.

Die Anzahl der Classen ungerader Zahlen nach dem Modul 2^λ ist $2^{\lambda-1}$. Nun ist aber für jede ungerade Zahl g, falls $\lambda > 2$ ist,

$$(1) \qquad g^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}.$$

Denn nehmen wir (1) als richtig an und setzen demgemäss

$$g^{2^{\lambda-2}} = 1 + h\,2^\lambda,$$

und erheben ins Quadrat, so folgt:

$$g^{2^{\lambda-1}} \equiv 1 \pmod{2^{\lambda+1}}.$$

Ist also die Formel (1) für λ richtig, so ist sie es auch für $\lambda + 1$, und da sie für $\lambda = 3$ gilt, so gilt sie allgemein. Daraus folgt, dass unter den Potenzen einer ungeraden Zahl g höchstens $2^{\lambda-2}$ nach dem Modul 2^λ verschiedene vorkommen können.

Andererseits folgt aber leicht für $g = 5$, dass $5^{2^{\lambda-2}}$ die niedrigste Potenz ist, die nach dem Modul 2^λ mit der Einheit congruent wird. Denn ist 5^e die niedrigste Potenz, die der Ein-

heit congruent ist, so ist e nach (1) ein Theiler von $2^{\lambda-2}$, also eine Potenz von 2, und wenn $e < 2^{\lambda-2}$ wäre, so müsste

$$5^{2^{\lambda-3}} \equiv 1 \pmod{2^\lambda}$$

sein. Dies ist aber nicht möglich, denn es gilt für jedes λ, was grösser als 2 ist, die Formel

$$5^{2^{\lambda-3}} = 1 + 2^{\lambda-1} h\ ^{1)}$$

mit ungeradem h, eine Formel, die sich ebenso wie die Formel (1) durch vollständige Induction beweisen lässt. Es sind also, wenn $\lambda \gtreqless 3$ ist, die $2^{\lambda-2}$ Potenzen

(2) $$1, 5, 5^2 \ldots 5^{2^{\lambda-2}-1}$$

nach dem Modul 2^λ alle von einander verschieden. Nun ist eine Relation von der Form $5^h \equiv -5^k$ für den Modul 4, also um so mehr für jede höhere Potenz von 2, unmöglich, und folglich sind die Grössen

(3) $$-1, -5, -5^2 \ldots -5^{2^{\lambda-2}-1}$$

nach dem Modul 2^λ sowohl unter einander als von den Grössen (2) verschieden, und da ihre gesammte Anzahl $2^{\lambda-1}$ beträgt, so ist jede ungerade Zahl einer und nur einer der Grössen (2), (3) nach dem Modul 2^λ congruent.

Setzen wir also

(4) $$a = 2, \quad b = 2^{\lambda-2},$$

so erhalten wir folgenden Satz für $\lambda \geqq 3$:

3. Für jede ungerade Zahl n lässt sich ein nach dem Modulpaar a, b völlig bestimmtes Zahlenpaar α, β angeben, so dass

$$n \equiv (-1)^\alpha\, 5^\beta \pmod{2^\lambda}$$

wird.

Der Fall $\lambda = 2$ kann hierunter mit subsumirt werden, weil dann $b = 1$ wird und $\beta = 0$ gesetzt werden kann. Um auch den Fall $\lambda = 1$ mit darunter zu begreifen, der aber kein besonderes Interesse bietet, müsste man $a = 1$, $b = 1$ setzen.

---

1) Wollte man an Stelle der Zahl 5 die Zahl 3 als Basis nehmen, so würde diese Formel für $\lambda = 3$ noch nicht gültig sein, wohl aber für jedes grössere λ, und daher könnte 3 als Basis ebenso gut dienen, wie 5. Der Grund für die Bevorzugung der Basis 5 liegt darin, dass alle Potenzen dieser Basis $\equiv 1 \pmod 4$ sind.

§. 16.

Die Gruppen der Zahlclassen nach einem zusammengesetzten Modul.

Aus der Verbindung der beiden Sätze 2. und 3. der beiden vorangegangenen Paragraphen ergiebt sich nun folgendes Resultat, durch welches die Aufgabe, die wir am Anfang des §. 14 gestellt haben, vollständig gelöst wird:

4. Wenn der Modul

$$m = 2^\lambda q_1^{\varkappa_1} q_2^{\varkappa_2} \dots$$

ist, und $g_1, g_2 \dots$ primitive Wurzeln der Quadrate der Primzahlen $q_1, q_2 \dots$ sind, wenn ferner

$$a = 2,\ b = \tfrac{1}{2}\varphi(2^\lambda),\ c_1 = \varphi(q_1^{\varkappa}),\ c_2 = \varphi(q_2^{\varkappa}) \dots$$

ist, so kann man für jede Zahl n, die zu m relativ prim ist, ein System von Zahlen $\alpha, \beta, \gamma_1, \gamma_2 \dots$ nach den Moduln $a, b, c_1, c_2 \dots$ eindeutig bestimmen, die den Gleichungen

$$(1)\qquad \begin{aligned} n &\equiv (-1)^\alpha 5^\beta \pmod{2^\lambda} \\ &\equiv g_1^{\gamma_1} \pmod{q_1^{\varkappa_1}} \\ &\equiv g_2^{\gamma_2} \pmod{q_2^{\varkappa_2}} \\ &\dots\dots\dots\dots \end{aligned}$$

genügen.

Die Zahlen $\alpha, \beta, \gamma_1, \gamma_2 \dots$ heissen das System der Indices von n für den Modul m.

Hier ist zunächst $\lambda \geqq 3$ vorausgesetzt. Der Satz gilt aber auch für die übrigen Werthe von λ, wenn

$$\text{für } \lambda = 0, 1,\quad a = 1,\quad b = 1$$
$$\text{„ } \lambda = 2,\quad a = 2,\quad b = 1$$

gesetzt wird. Für $\lambda = 0, 1$ sind die Indices α und $\beta = 0$ zu setzen oder auch ganz wegzulassen, für $\lambda = 2$ fällt β weg, während α gleich 0 oder gleich 1 sein kann.

Um nun also die Gruppe $\mathfrak{N}$ der Zahlclassen N nach dem Modul m durch eine Basis darzustellen, bestimme man die Zahlclassen

$$(2)\qquad A, B, C_1, C_2 \dots,$$

oder wenigstens Repräsentanten dieser Classen, was immer möglich ist, aus den Congruenzen

$$\begin{array}{llll}
A \equiv -1 \pmod{2^\lambda} & \equiv 1 \pmod{q_1^{\varkappa_1}} & \equiv 1 \pmod{q_2^{\varkappa_2}} & \ldots \\
B \equiv 5 \quad " & \equiv 1 \quad " & \equiv 1 \quad " & \ldots \\
C_1 \equiv 1 \quad " & \equiv g_1 \quad " & \equiv 1 \quad " & \ldots \\
C_2 \equiv 1 \quad " & \equiv 1 \quad " & \equiv g_2 \quad " & \ldots \\
\cdots & \cdots & \cdots & \cdots
\end{array}$$

und nach 4. erhält man dann für jede Zahl n unserer Gruppe

(3) $$n \equiv A^\alpha B^\beta C_1^{\gamma_1} C_2^{\gamma_2} \ldots \pmod{m}.$$

Die A, B, C_1, C_2 ... sind also die Elemente einer Basis der Gruppe $\mathfrak{R}$ von den Graden a, b, c_1, c_2 ...

Wenn m ungerade oder nur durch die erste Potenz von 2 theilbar ist, so fallen aus der Basis die beiden Elemente A, B weg. Ist m durch 4, aber nicht durch 8 theilbar, so fällt B weg und das Element A vom zweiten Grade bleibt.

5. Zerlegt man die Zahlen a, b, c_1, c_2 ... in Potenzen von einander verschiedener Primzahlen, so erhält man die Invarianten der Gruppe $\mathfrak{R}$.

Um die verschiedenen Fälle zusammenzufassen, bezeichnen wir die Elemente der Basis (2) mit

(4) $$C_{-1}, C_0, C_1 \ldots C_\mu.$$

Hierin sollen C_{-1}, C_0 für A und B stehen und sind also gleich 1 zu setzen, wenn $\lambda = 0$ oder $\lambda = 1$ ist. Wenn $\lambda = 2$ ist, so ist $B = C_{-1} = 1$, $A = C_0$, und wenn $\lambda > 1$ ist, $A = C_{-1}$, $B = C_0$ zu setzen.

Die Grade dieser Elemente seien mit

(5) $$c_{-1}, c_0, c_1 \ldots c_\mu$$

bezeichnet, und die Indices einer Zahl aus $\mathfrak{R}$, die nach den Grössen (5) als Moduln zu nehmen sind, mit

(6) $$\nu_{-1}, \nu_0, \nu_1 \ldots \nu_\mu.$$

Ist $\lambda = 0$ oder 1, so haben ν_{-1} und ν_0 nur den Werth 0, ist $\lambda = 2$, so hat ν_{-1} den Werth 0 und ν_0 den Werth 0 oder 1. Ist $\lambda \geqq 3$, so hat ν_{-1} einen der beiden Werthe 0, 1, und ν_0 einen der Werthe 0, 1, 2, ... $c_0 - 1$; μ ist immer gleich der Anzahl der von einander verschiedenen ungeraden Primzahlen, die in m aufgehen. Wir wollen, indem wir ν_{-1}, c_{-1} bei Seite lassen, ν_0, ν_1 ... ν_μ die den Primzahlen 2, q_1 ... q_μ entsprechenden Indices von n und c_0, c_1 ... c_μ die denselben Primzahlen entsprechenden Indexmoduln nennen. Diese Indexmoduln sind

$$c_0 = \varphi(2^{\lambda-1}), \quad c_1 = \varphi(q_1^{\varkappa_1}), \ldots c_\mu = \varphi(q_\mu^{\varkappa_\mu}),$$

und nur wenn $\lambda = 2$ ist, ist $c_0 = 2$ und nicht $= 1$ zu setzen.

Wenn wir dann mit $\varepsilon_{-1}, \varepsilon_0, \varepsilon_1 \dots \varepsilon_\mu$ ein System primitiver Einheitswurzeln der Grade $c_{-1}, c_0, c_1 \dots c_\mu$ bezeichnen, und mit $\beta_{-1}, \beta_0, \beta_1 \dots \beta_\mu$ die Indices einer Zahl b, so erhalten wir die Charaktere der Gruppe $\mathfrak{N}$ in der Form

$$(7) \qquad \chi_b(n) = \varepsilon_{-1}^{\beta_{-1}\nu_{-1}} \varepsilon_0^{\beta_0\nu_0} \varepsilon_1^{\beta_1\nu_1} \dots \varepsilon_\mu^{\beta_\mu\nu_\mu}.$$

Darin ist $\varepsilon_{-1} = 1$, wenn $\lambda = 0, 1, 2$ ist; in den anderen Fällen ist $\varepsilon_{-1} = -1$, und $\varepsilon_1, \dots \varepsilon_\mu$ sind primitive Einheitswurzeln der Grade

$$c_1 = \varphi(q_1^{\varkappa_1}), \dots c_\mu = \varphi(q_\mu^{\varkappa_\mu}).$$

Dritter Abschnitt.

Die Gruppe der Kreistheilungskörper.

---

§. 17.

Die Resolventen der Kreistheilungstheorie.

Von den Sätzen über Abel'sche Gruppen machen wir eine Anwendung auf die Kreistheilungstheorie für den Fall, dass der Grad der Einheitswurzeln nicht eine Primzahl, sondern eine höhere Potenz einer Primzahl ist. Ist q eine ungerade Primzahl und $m = q^\varkappa$, $\varkappa > 1$, so nehmen wir eine primitive Congruenzwurzel g von m und setzen für jede durch q nicht theilbare Zahl n

(1) $$n \equiv g^\nu \pmod{m}.$$

Dann ist ν der **Index** von n. Durchläuft n die Gruppe $\mathfrak{N}$ der durch q nicht theilbaren Zahlclassen nach dem Modul m vom Grade

(2) $$c = \varphi(q^\varkappa) = q^{\varkappa-1}(q-1),$$

so durchläuft ν ein volles Restsystem nach dem Modul c. Wir nehmen nun eine primitive m^{te} Einheitswurzel r und eine primitive c^{te} Einheitswurzel ε und bilden die **Lagrange'schen Resolventen**

(3) $$(\varepsilon^\beta, r) = \sum^{n} \varepsilon^{\beta\nu} r^n,$$

worin β ein beliebiger Exponent ist. Es handelt sich um die Frage, wann eine solche Resolvente verschwinden kann. Ist $\varkappa = 1$, also m eine Primzahl, so verschwindet sie, wie wir im Bd. I, §. 169 gesehen haben, für keinen Werth von β. Im allgemeinen Falle eines beliebigen $\varkappa$ bedeute n' eine beliebige Zahl aus $\mathfrak{N}$. Dann durchläuft $n n'$ zugleich mit n die ganze Gruppe $\mathfrak{N}$. Man kann also in (3) n durch $n n'$ ersetzen, wenn man zugleich

ν durch $\nu + \nu'$ ersetzt, wenn ν' den Index von n' bedeutet. Dadurch folgt aus (3):

$$\varepsilon^{-\beta\nu'}(\varepsilon^{\beta}, r) = \sum^{n} \varepsilon^{\beta\nu} r^{nn'},$$

und wenn man also mit $r^{n'}$ multiplicirt und die Summe über n' nimmt:

(4) $$(\varepsilon^{-\beta}, r)(\varepsilon^{\beta}, r) = \sum^{n, n'} \varepsilon^{\beta\nu} r^{n'(n+1)}.$$

Es ist also zunächst die Summe

(5) $$\sigma = \sum^{n'} r^{n'(n+1)}$$

zu bestimmen. Die Summe σ verschwindet aber immer, wenn $n + 1$ nicht durch $q^{\varkappa-1}$ theilbar ist (nach Bd. I, §. 133); denn dann ist r^{n+1} eine Einheitswurzel, deren Grad eine höhere als die erste Potenz von q ist. σ kann also nur dann von Null verschieden sein, wenn n die Form hat

(6) $$n \equiv -1 + t q^{\varkappa-1} \pmod{m},$$

und dann wollen wir seinen Werth mit σ_t bezeichnen. Wir erhalten alle Werthe von n nach dem Modul m, die in der Form (6) enthalten sind, wenn wir t ein volles Restsystem nach dem Modul q durchlaufen lassen, also etwa

(7) $$t = 0, 1, 2 \ldots q - 1$$

setzen. Die Summe σ besteht aus $\varphi(m)$ Gliedern. Ist $t = 0$, so wird jedes dieser Glieder $= 1$ und es folgt

(8) $$\sigma_0 = \varphi(m) = q^{\varkappa} - q^{\varkappa-1};$$

für jeden anderen Werth von t ist r^{n+1} eine primitive q^{te} Einheitswurzel, und in σ_t kommt dann jede solche Einheitswurzel $\varphi(m) : (q - 1) = q^{\varkappa-1}$ mal vor. Die Summe aller primitiven q^{ten} Einheitswurzeln ist aber gleich -1 und also folgt für $t = 1, 2 \ldots q - 1$

(9) $$\sigma_t = -q^{\varkappa-1}.$$

Damit ist die Summe σ bestimmt.

Um aber den Werth der Summe in (4) daraus abzuleiten, ist es noch nöthig, den Index ν der Zahlen n von der Form (6) zu ermitteln.

Für diese Zahlen ist aber

$$g^{\nu} \equiv -1 \pmod{q^{\varkappa-1}},$$

und da nach dem Fermat'schen Satze [§. 14. (11)]

(10) $$g^{\frac{1}{2}\varphi(q^{\varkappa})} \equiv -1 \pmod{q^{\varkappa}}$$

ist, so folgt

$$g^{\nu} \equiv g^{\frac{1}{2}\varphi(q^{\varkappa})} \pmod{q^{\varkappa-1}};$$

also $\nu \equiv \frac{1}{2}\varphi(q^{\varkappa})$ $[\mathrm{mod}\ \varphi(q^{\varkappa-1})]$, da der Index einer Zahl für den Modul $q^{\varkappa-1}$ völlig bestimmt ist nach dem Modul $\varphi(q^{\varkappa-1})$. Es wird also

(11) $$\nu \equiv \frac{1}{2}\varphi(q^{\varkappa}) + \tau\varphi(q^{\varkappa-1})\ [\mathrm{mod}\ \varphi(q^{\varkappa})],$$

und hierin durchläuft nun, da $\varphi(q^{\varkappa}) = q\,\varphi(q^{\varkappa-1})$ ist, τ zugleich mit t ein volles Restsystem nach dem Modul q. Dem Werthe $t = 0$ entspricht der Werth $\tau = 0$ wegen (10).

Es ist aber

$$\varepsilon^{\frac{1}{2}\varphi(q^{\varkappa})} = -1, \quad \varepsilon^{\varphi(q^{\varkappa-1})} = \varrho,$$

wenn ϱ eine primitive q^{te} Einheitswurzel ist, also nach (11)

$$\varepsilon^{\nu} = -\varrho^{\tau},$$

und danach ergiebt sich aus (8) und (9):

$$(\varepsilon^{-\beta}, r)\,(\varepsilon^{\beta}, r) = \sum \varepsilon^{\beta\nu}\sigma_t$$
$$= (-1)^{\beta}(q^{\varkappa} - q^{\varkappa-1}) - (-1)^{\beta}q^{\varkappa-1}\sum_{1,\,q-1}^{\tau}\varrho^{\tau\beta}.$$

Nun hat die Summe $\sum\limits_{1,\,q-1}^{\tau}\varrho^{\tau\beta}$, wenn β nicht durch q theilbar ist, den Werth -1, und wenn β durch q theilbar ist, den Werth $q - 1$, so dass man folgendes Resultat erhält:

(12) $$\begin{aligned}(\varepsilon^{-\beta}, r)\,(\varepsilon^{\beta}, r) &= 0, & \beta &\equiv 0 \pmod{q}\\ &= (-1)^{\beta}q^{\varkappa}, & \beta &\text{ nicht} \equiv 0 \pmod{q}.\end{aligned}$$

Wenn also β nicht durch q theilbar ist, so kann von den Factoren $(\varepsilon^{-\beta}, r)$, (ε^{β}, r) keiner verschwinden; wenn aber β durch q theilbar ist, so verschwindet wenigstens einer der beiden Factoren. Dass sie dann beide verschwinden, zeigt die folgende directe Betrachtung der Summe.

Wenn β durch q theilbar ist, so ist für jedes ganzzahlige t

$$\varepsilon^{\beta[\nu + t\varphi(q^{\varkappa-1})]} = \varepsilon^{\beta\nu}$$

$$g^{t\varphi(q^{\varkappa-1})} \equiv 1 + \tau q^{\varkappa-1} \pmod{q^{\varkappa}},$$

worin nun τ zugleich mit t ein volles Restsystem nach dem Modul q durchläuft. Wenn man also in (3) unter der Voraussetzung, dass β durch q theilbar sei, ν durch $\nu + t\varphi(q^{\varkappa-1})$, d. h. n durch $n(1 + \tau q^{\varkappa-1})$ ersetzt, so folgt

$$(\varepsilon^{\beta}, r) = \sum^{n} \varepsilon^{\beta\nu} r^{n} r^{n q^{\varkappa-1}\tau}.$$

Diese Summe ist also von dem willkürlich anzunehmenden τ unabhängig. Summirt man hier von $\tau = 0$ bis $\tau = q - 1$, so ergiebt sich, da $\sum r^{n q^{\varkappa - 1}\tau} = 0$ ist:

(13) $$(\varepsilon_i^\beta, r) = 0.$$

Wir haben also den Satz:

1. **Ist der Grad der Einheitswurzel r eine Potenz einer ungeraden Primzahl, so verschwindet die Resolvente (ε_i^β, r) dann und nur dann, wenn β durch q theilbar ist.**

Wir haben noch den Fall zu betrachten, dass der Grad der Einheitswurzel r eine Potenz von 2 ist. Wir setzen also

$$m = 2^\lambda$$

und nehmen zunächst $\lambda \geqq 3$ an. Dann können wir für jede ungerade Zahl n ein Indexpaar ν, ν_1 aus den Congruenzen

$$n \equiv (-1)^{\nu_1} 5^\nu \pmod m$$

bestimmen, und zwar ist ν_1 nach dem Modul 2, ν nach dem Modul $2^{\lambda - 2}$ bestimmt. Unter den Resolventen verstehen wir in diesem Falle die Summen

(14) $$\left((-1)^{\beta_1}, \Theta^\beta, r\right) = \sum^n (-1)^{\beta_1 \nu_1} \Theta^{\beta\nu} r^n,$$

worin Θ eine primitive Einheitswurzel vom Grade $2^{\lambda-2}$ bedeutet. Nun verfahren wir ganz ähnlich wie vorher. Wenn wir in (14) n durch nn' ersetzen und mit ν_1', ν' die Indices von n' bezeichnen, so ergiebt sich

(15) $$(-1)^{-\beta_1 \nu_1'} \Theta^{-\beta\nu'} \left((-1)^{\beta_1}, \Theta^\beta, r\right) = \sum^n (-1)^{\beta_1 \nu_1} \Theta^{\beta\nu} r^{nn'},$$

und daraus durch Multiplication mit $r^{n'}$ und Summation nach n'

(16) $$\left((-1)^{-\beta_1}, \Theta^{-\beta}, r\right) \left((-1)^{\beta_1}, \Theta^\beta, r\right) = \sum^{n n'} (-1)^{\beta_1 \nu_1} \Theta^{\beta\nu} r^{n'(n+1)}.$$

Nun ist aber aus den oben angeführten Gründen

$$\sum^{n'} r^{n'(n+1)} = 0, \text{ wenn } n+1 \text{ nicht durch } 2^{\lambda-1} \text{ theilbar ist,}$$
$$= 2^{\lambda-1} \text{ für } n+1 \equiv 0 \pmod{2^\lambda},\ \nu = 0,\ \nu_1 = 1,$$
$$= -2^{\lambda-1} \text{ für } n+1 \equiv 2^{\lambda-1} \pmod{2^\lambda},\ \nu = 2^{\lambda-3},\ \nu_1 = 1,$$

und danach giebt (16)

(17) $$\left((-1)^{-\beta_1}, \Theta^{-\beta}, r\right) \left((-1)^{\beta_1}, \Theta^\beta, r\right) = (-1)^{\beta_1} 2^\lambda,\ \beta \equiv 1 \pmod 2$$
$$= 0 \quad ,\ \beta \equiv 0 \pmod 2.$$

Dass im Falle eines geraden β jeder der beiden Factoren verschwindet, sieht man, wenn man in (15)

$$n' = 1 + 2^{\lambda-1},$$

also

$$r^{n'} = -r, \quad \nu_1' = 0, \quad \nu' = 2^{\lambda-3}$$

setzt. Dann giebt diese Formel, da n ungerade ist:

$$\left((-1)^{\beta_1}, \Theta^{\beta}, r\right) = -\Theta^{\beta 2^{\lambda-3}}\left((-1)^{\beta_1}, \Theta^{\beta}, r\right).$$

Bei geradem β ist aber $\Theta^{\beta 2^{\lambda-3}} = +1$ und folglich:

(18) $$\left((-1)^{\beta_1}, \Theta^{\beta}, r\right) = 0;$$

also:

2. Ist der Grad der Einheitswurzel r eine Potenz von 2 und grösser als 4, so verschwindet die Resolvente $\left((-1)^{\beta_1}, \Theta^{\beta}, r\right)$ dann und nur dann, wenn β gerade ist.

Im Falle $m = 4$, also $r = i$, hat man nur die zwei Resolventen $i + i^3$, $i - i^3$, die wir unter der Bezeichnung $\left((-1)^{\beta}, i\right)$, $\beta = 0, 1$ zusammenfassen können, und es ist $\left((-1)^{\beta}, i\right)$ dann und nur dann $= 0$, wenn $\beta = 0$ ist.

§. 18.

Kreistheilungskörper.

Die Theorie der Abel'schen Gruppen eröffnet uns einen tieferen Einblick in die Theorie der Einheitswurzeln und der daraus entspringenden algebraischen Zahlen.

Es möge jetzt m irgend eine ganze positive Zahl sein, die in ihre Primfactoren zerlegt sei:

(1) $$m = 2^{\lambda} q_1^{\varkappa_1} q_2^{\varkappa_2} \ldots,$$

und es sei r eine primitive m^{te} Einheitswurzel. Den Fall $\lambda = 1$ können wir ein- für allemal von unserer Betrachtung ausschliessen; denn wenn m ungerade ist und r die primitiven m^{ten} Einheitswurzeln durchläuft, so kommen darunter keine zwei entgegengesetzte vor, und $-r$ durchläuft die primitiven $2m^{\text{ten}}$ Einheitswurzeln.

r ist die Wurzel einer ganzzahligen irreduciblen Abel'schen Gleichung vom Grade

(2) $$\nu = \varphi(m),$$

wie wir im §. 134 des ersten Bandes nachgewiesen haben.

Der Inbegriff aller rationalen Functionen von r mit rationalen Zahlen als Coëfficienten ist also ein Zahlkörper $\Omega(r)$ vom Grade ν, den wir einen Kreistheilungskörper nennen. Wir wollen aber den Begriff des Kreistheilungskörpers noch etwas allgemeiner fassen und darunter jeden Körper verstehen, dessen Zahlen lauter rationale Functionen irgend welcher Einheitswurzeln sind.

Den Körper ν^{ten} Grades $\Omega(r)$, der aus allen rationalen Functionen einer m^{ten} Einheitswurzel r besteht, nennen wir zur genaueren Unterscheidung den vollen Kreistheilungskörper der Ordnung m und bezeichnen ihn mit Ω_m.

Beliebige Einheitswurzeln $r, r', r'' \ldots$ beliebiger Grade $m, m', m'' \ldots$ kann man immer auffassen als Potenzen einer und derselben Einheitswurzel ϱ, deren Grad das kleinste gemeinschaftliche Vielfache von $m, m', m'' \ldots$ ist. Demnach ist ein Kreistheilungskörper, der nur rationale Functionen von $r, r', r'' \ldots$ enthält, ein Theiler des vollen Kreistheilungskörpers $\Omega(\varrho)$, und wir bekommen also alle überhaupt existirenden Kreistheilungskörper, wenn wir die sämmtlichen Divisoren aller vollen Kreistheilungskörper aufsuchen.

Die Galois'sche Gruppe des Körpers Ω_m besteht aus den sämmtlichen Substitutionen

$$(3) \qquad (r, r^n),$$

wenn n jede nach dem Modul m genommene relative Primzahl zu m bedeutet. Denn die Kreistheilungsgleichung ν^{ten} Grades, deren Wurzeln die r^n sind, ist eine Normalgleichung und also ihre eigene Galois'sche Resolvente. Da, wenn a, b zwei dieser Zahlen n sind,

$$(r, r^a)\,(r, r^b) = (r, r^{ab})$$

ist, so ist diese Gruppe isomorph mit der Gruppe $\mathfrak{N}$ aller Zahlclassen N der zu m theilerfremden Zahlen, die wir im vorigen Paragraphen betrachtet haben.

Ist $\mathfrak{A}$ ein Theiler von $\mathfrak{N}$, und ϱ eine zu $\mathfrak{A}$ gehörige Function aus Ω_m, so ist der Inbegriff der rationalen Functionen von ϱ, $\Omega(\varrho)$, ein in Ω_m enthaltener Körper.

Ist umgekehrt Ω ein Theiler von Ω_m und ϱ eine primitive Zahl des Körpers Ω, also auch eine Zahl in Ω_m, so kann Ω als der Inbegriff der rationalen Functionen von ϱ dargestellt und mit $\Omega(\varrho)$ bezeichnet werden.

Diese Function ϱ gehört dann zu einer gewissen Gruppe $\mathfrak{A}$, die ein Theiler von $\mathfrak{R}$ ist. Wir nennen auch die Gruppe $\mathfrak{A}$ und den Körper $\Omega(\varrho)$ zusammengehörig und ziehen daraus den Satz:

1. Zu jedem Theiler $\mathfrak{A}$ von $\mathfrak{R}$ gehört ein gewisser in Ω_m enthaltener Kreistheilungskörper $\Omega(\varrho)$, und umgekehrt gehört zu jedem Theiler $\Omega(\varrho)$ von Ω_m ein gewisser Theiler $\mathfrak{A}$ von $\mathfrak{R}$ als Gruppe, in dem Sinne, dass, wenn a eine Zahl aus $\mathfrak{A}$ ist, alle Zahlen des Körpers $\Omega(\varrho)$ die Permutationen (r, r^a) gestatten, und dass umgekehrt jede Zahl in Ω_m, die diese Permutationen gestattet, in $\Omega(\varrho)$ enthalten ist.

Die Galois'sche Gruppe eines solchen Körpers $\Omega(\varrho)$ erhalten wir nach Bd. I, §. 156, wenn wir $\mathfrak{R}$ in das System der Nebengruppen zerlegen:

$$\mathfrak{R} = \mathfrak{A} + \mathfrak{A}_1 + \mathfrak{A}_2 + \cdots,$$

und die unter den Nebengruppen $\mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2 \ldots$ durch Composition mit den Elementen von $\mathfrak{R}$ hervorgerufenen Permutationen aufsuchen. Diese Gruppe ist aber nach §. 4 isomorph mit der Gruppe $\mathfrak{R}/\mathfrak{A}$, also auch isomorph mit der zu $\mathfrak{A}$ reciproken Gruppe (§. 12), die wir mit $\mathfrak{B}$ bezeichnen wollen. Ist a der Grad von $\mathfrak{A}$ und b der von $\mathfrak{B}$, so ist $ab = \nu$, und ϱ genügt einer irreduciblen Abel'schen Gleichung vom Grade b.

2. Wir bekommen also alle Kreistheilungskörper, wenn wir zu jedem Modul m die sämmtlichen Divisoren $\mathfrak{A}$ der Gruppe $\mathfrak{R}$ bilden, zu jeder dieser Gruppen $\mathfrak{A}$ eine zugehörige Function ϱ suchen und daraus die Körper $\Omega(\varrho)$ ableiten.

Es ist aber noch die Frage, ob bei diesem Processe ein und derselbe Körper Ω mehrmals auftreten kann, wodurch wir auf die Untersuchung der gemeinschaftlichen Theiler zweier Kreistheilungskörper geführt werden.

Nach der oben gegebenen Definition ist wohl zu unterscheiden zwischen der Gruppe, zu der ein Körper Ω gehört, und der Galois'schen Gruppe des Körpers; beide Gruppen sind zu einander reciprok. So gehört der Körper Ω_m selbst zur Einheitsgruppe, während seine Galois'sche Gruppe $\mathfrak{R}$ ist.

Es gilt nun der Satz:

3. **Sind Ω' und Ω'' zwei Theiler von Ω_m, die zu den Gruppen $\mathfrak{A}'$ und $\mathfrak{A}''$ gehören, so ist Ω'' dann und nur dann ein Theiler von Ω', wenn $\mathfrak{A}'$ ein Theiler von $\mathfrak{A}''$ ist.**

Denn wenn Ω'' ein Theiler von Ω' ist, so müssen alle Zahlen von Ω'' die Substitutionen der Gruppe $\mathfrak{A}'$, zu der Ω' gehört, gestatten, also muss $\mathfrak{A}'$ in $\mathfrak{A}''$ enthalten sein. Und wenn umgekehrt $\mathfrak{A}'$ in $\mathfrak{A}''$ enthalten ist, so gestatten alle Zahlen von Ω'' die sämmtlichen Substitutionen von $\mathfrak{A}'$ und sind also rational durch eine primitive Zahl des Körpers Ω' darstellbar; d. h. Ω'' ist in Ω' enthalten (§. 144 des ersten Bandes).

Der Körper Ω_m enthält als Theiler alle Körper Ω_{m_1}, bei denen m_1 ein Theiler von m ist; denn Ω_{m_1} besteht aus allen rationalen Functionen von $r^{\frac{m}{m_1}}$. Nun ist dann und nur dann

$$r^{a\frac{m}{m_1}} = r^{\frac{m}{m_1}},$$

wenn

$$a \equiv 1 \pmod{m_1}. \tag{4}$$

Die Zahlen a aus $\mathfrak{R}$, die der Congruenz (4) genügen, bilden also die Gruppe, zu der der Körper Ω_{m_1} gehört. Wir wollen diese Gruppe mit $\mathfrak{A}_{m_1}$ bezeichnen und symbolisch

$$\mathfrak{A}_{m_1} \equiv 1 \pmod{m_1}. \tag{5}$$

setzen. Da der Grad des Körpers Ω_{m_1} gleich $\varphi(m_1)$ ist, was zugleich der Index des Theilers $\mathfrak{A}_{m_1}$ von $\mathfrak{R}$ ist, so ist der Grad von $\mathfrak{A}_{m_1}$ gleich $\varphi(m) : \varphi(m_1)$.

Ist $m = m_1 m_2$ und m_1 relativ prim zu m_2, so erhält man alle Zahlen von $\mathfrak{A}_{m_1}$ aus $a = 1 + x m_1$, wenn man x so bestimmt, dass a nach dem Modul m_2 mit allen relativen Primzahlen zu m_2 congruent wird. Daraus ergiebt sich in Uebereinstimmung mit der obigen allgemeinen Bestimmung der Grad von $\mathfrak{A}_{m_1}$ für diesen Fall $= \varphi(m_2)$.

Sind nun aber m_1 und m_2 irgend zwei Theiler von m, und μ der grösste gemeinschaftliche Theiler von m_1 und m_2, so wird der grösste gemeinschaftliche Theiler der beiden Körper Ω_{m_1}, Ω_{m_2} zu der Gruppe gehören, die man als kleinstes gemeinschaftliches Vielfaches der beiden Gruppen

$$\mathfrak{A}_{m_1} \equiv 1 \pmod{m_1}, \quad \mathfrak{A}_{m_2} \equiv 1 \pmod{m_2} \tag{6}$$

erhält. Das ist aber die Gruppe

(7) $$\mathfrak{A}_\mu \equiv 1 \pmod{\mu},$$

d. h. die Gruppe, die aus allen den Zahlen von $\mathfrak{R}$ besteht, die der Congruenz $a \equiv 1 \pmod{\mu}$ genügen. Denn zunächst ist klar, dass $\mathfrak{A}_{m_1}$ und $\mathfrak{A}_{m_2}$ Divisoren von $\mathfrak{A}_\mu$ sind. Also ist auch das kleinste gemeinschaftliche Vielfache von $\mathfrak{A}_{m_1}$ und $\mathfrak{A}_{m_2}$ in $\mathfrak{A}_\mu$ enthalten. Ist aber andererseits $\alpha = 1 + \xi\,\mu$ irgend eine Zahl in $\mathfrak{A}_\mu$, so kann man die Zahlen $a_1 = 1 + x_1 m_1$ in $\mathfrak{A}_{m_1}$ und $a_2 = 1 + x_2 m_2$ in $\mathfrak{A}_{m_2}$ so bestimmen, dass $\alpha \equiv a_1 a_2 \pmod{m}$ wird. Man hat nur $\xi\,\mu = x_1 m_1 + x_2 m_2$ zu setzen, was nach Bd. I, §. 118 immer möglich ist. Es ist also auch $\mathfrak{A}_\mu$ in dem kleinsten gemeinschaftlichen Vielfachen von $\mathfrak{A}_{m_1}$ und $\mathfrak{A}_{m_2}$ enthalten, welches demnach $\mathfrak{A}_\mu$ selbst ist. Daraus also der Satz:

4. Sind m_1 und m_2 irgend zwei natürliche Zahlen und μ der grösste gemeinschaftliche Theiler von m_1 und m_2, so ist der Körper Ω_μ der grösste gemeinschaftliche Theiler von Ω_{m_1} und Ω_{m_2} und $\Omega_{\frac{m_1 m_2}{\mu}}$ ihr kleinstes gemeinsames Multiplum.

Daraus folgt nun: wenn zwei volle Kreistheilungskörper Ω_m und $\Omega_{m'}$ einen gemeinsamen Theiler Ω haben, und m' ist kleiner als m, so muss es einen echten Theiler d von m geben, so dass Ω auch ein Theiler von Ω_d ist.

Wir wollen einen Theiler von Ω_m primär nennen, wenn er nicht zugleich in einem vollen Kreistheilungskörper $\Omega_{m'}$ von niedrigerem m' enthalten ist. Dann folgt also, dass man alle nicht primären Theiler von Ω_m erhält, wenn man in Ω_d den Index d alle echten Theiler von m durchlaufen lässt und die Theiler von Ω_d aufsucht.

Bezeichnen wir nun mit $q_1, q_2, \ldots q_\tau$ die sämmtlichen in m aufgehenden verschiedenen Primzahlen (2 eingeschlossen) und setzen

(8) $$m = q_1 m_1 = q_2 m_2 = \cdots = q_\tau m_\tau,$$

so ist jedes d Theiler von einem der $m_1, m_2, \ldots m_\tau$, und wir erhalten die nicht primären Theiler von Ω_m, wenn wir alle Theiler der Körper

(9) $$\Omega_{m_1}, \Omega_{m_2}, \ldots \Omega_{m_\tau}$$

aufsuchen. Diese Körper gehören aber zu der Gruppe

(10) $$Q_1 \equiv 1 \pmod{m_1},\ Q_2 \equiv 1 \pmod{m_2}, \ldots Q_\tau \equiv 1 \pmod{m_\tau},$$

und also wird nach 3. ein Theiler Ω von Ω_m dann und nur dann nicht primär sein, wenn in der zu Ω gehörigen Gruppe $\mathfrak{A}$ eine der Gruppen $Q_1, Q_2, \ldots Q_r$ enthalten ist. Wenn wir also solche Theiler der Gruppe $\mathfrak{R}$, die keine der Gruppen $Q_1, Q_2 \ldots Q_r$ als Theiler enthalten, primäre Theiler nennen, so können wir den Satz aussprechen:

5. Um alle primären Theiler von Ω_m zu erhalten, hat man alle primären Theiler der Gruppe $\mathfrak{R}$ aufzusuchen und die zugehörigen Körper zu bilden.

6. Wenn man aber alle primären Theiler aller vollen Kreistheilungskörper aufstellt, so erhält man jeden Kreistheilungskörper, und jeden nur einmal, und zwar jeden dargestellt durch Einheitswurzeln möglichst niedrigen Grades.

Der Körper Ω_{2m} hat, wenn m ungerade ist, gar keinen primären Theiler und ist mit Ω_m identisch. In allen anderen Fällen ist Ω_m wenigstens sein eigener primärer Theiler.

Es ist für das Folgende noch erforderlich, dass wir uns über den Umfang und die Constitution der Gruppen Q klar werden.

§. 19.

Primäre und nicht primäre Theiler der Gruppe $\mathfrak{R}$.

Wir bezeichnen mit q irgend eine der in m aufgehenden Primzahlen und setzen $m = q\,m'$. Dann betrachten wir die Gruppe

$$Q \equiv 1 \pmod{m'}.$$

Um die Bedingungen für eine Zahl in Q zu ermitteln, wenden wir die Darstellung der Gruppe $\mathfrak{R}$ durch eine Basis und die Bezeichnungsweise der Indices an, wie wir sie im §. 16 eingeführt und erklärt haben, und bezeichnen danach die zu Q reciproke Gruppe mit P.

Die Indices einer Zahl in Q bezeichnen wir mit

$$\gamma_{-1}, \gamma_0, \gamma_1, \ldots \gamma_\mu,$$

und einer Zahl in P mit

$$\delta_{-1}, \delta_0, \delta_1, \ldots \delta_\mu.$$

Dann müssen die γ der Bedingung genügen:

(1) $$C_{-1}^{\gamma-1}\, C_0^{\gamma_0}\, C_1^{\gamma_1} \ldots C_\mu^{\gamma_\mu} \equiv 1 \pmod{m'}.$$

Diese Bedingung fordert, dass alle Indices mit Ausnahme des der Primzahl q entsprechenden, den wir mit γ bezeichnen, Null sein müssen. In Bezug auf γ ist aber zu unterscheiden, ob q noch in m' aufgeht oder nicht, d. h. ob q ein mehrfacher oder nur ein einfacher Factor von m ist. Ist q nicht mehr in m' enthalten, so enthält die Congruenz (1) gar keine Beschränkung für γ, und γ kann jeden Werth nach dem Modul c, d. h. jeden Werth $0, 1, \ldots q-2$ annehmen.

Ist aber q noch in m' enthalten, also m durch $q^\varkappa$ theilbar, und $\varkappa > 1$, so fordert die Bedingung (1):

$$C^\gamma \equiv 1 \pmod{q^{\varkappa-1}},$$

also

(2) $$\gamma \equiv 0 \left(\bmod \frac{c}{q}\right),$$

und γ kann also jeden der Werthe

$$0, \frac{c}{q}, \frac{2c}{q}, \ldots \frac{(q-1)c}{q}$$

erhalten. Im ersten Falle ist der Grad der Gruppe Q gleich $q-1$, im zweiten gleich q.

Die Indices δ einer Zahl aus der Gruppe P erhält man nach §. 12, 7. und §. 16, (7) aus der Bedingung, dass für alle zulässigen γ

(3) $$\varepsilon_{-1}^{\gamma-1\,\delta-1}\, \varepsilon_0^{\gamma_0\delta_0}\, \varepsilon_1^{\gamma_1\delta_1} \ldots \varepsilon_\mu^{\gamma_\mu\delta_\mu} = 1$$

sein soll. Nach dem, was eben über die Indices γ bewiesen ist, fordert aber (3) nur das eine, dass der der Primzahl q entsprechende Index δ durch q oder durch $q-1$ theilbar sein soll, je nachdem q mehrmals oder nur einmal in m aufgeht. Wir heben also den Satz hervor:

7. Die zu Q reciproke Gruppe P ist dadurch charakterisirt, dass der q entsprechende Index δ aller seiner Zahlen durch q oder durch $q-1$ theilbar ist, je nachdem q mehrmals oder nur einmal in m aufgeht.

Und daraus:

8. Ein nicht primärer Theiler $\mathfrak{A}$ von $\mathfrak{R}$ ist dadurch charakterisirt, dass in der reciproken Gruppe $\mathfrak{B}$

der einer Primzahl q entsprechende Index β aller Zahlen b durch q oder durch $q-1$ theilbar ist, je nachdem q mehrmals oder nur einmal unter den Primfactoren von m vorkommt.

§. 20.

Die Kreistheilungsperioden.

Als die einfachsten Functionen, durch die man die Kreistheilungskörper darzustellen versuchen kann, bieten sich die Kreistheilungsperioden dar, die eine unmittelbare Verallgemeinerung der im §. 167 des ersten Bandes betrachteten Gauss'schen Perioden sind. Wir verstehen darunter Folgendes.

Es bedeute $\mathfrak{A}$ einen Theiler der Gruppe $\mathfrak{N}$ vom Index e und a durchlaufe die Zahlen von $\mathfrak{A}$. Ist r eine primitive m^{te} Einheitswurzel, so heisst die Summe

$$(1) \qquad \eta = \sum^{a} r^{a}$$

eine zu der Gruppe $\mathfrak{A}$ gehörige Kreistheilungsperiode vom Index e.

Machen wir in (1) eine der Substitutionen (r, r^a), so bleibt η ungeändert, wie unmittelbar aus der Gruppeneigenschaft der a folgt.

Um $\mathfrak{N}$ in die zu $\mathfrak{A}$ gehörigen Nebengruppen zu zerlegen, müssen wir die Zahlen $1, n_1, n_2, \ldots n_{e-1}$ aus $\mathfrak{N}$ passend auswählen, dass man

$$(2) \qquad \mathfrak{N} = \mathfrak{A} + \mathfrak{A} n_1 + \mathfrak{A} n_2 + \cdots + \mathfrak{A} n_{e-1}$$

erhält. Machen wir dann in η die Substitutionen

$$(3) \qquad (r, r), (r, r^{n_1}), \ldots (r, r^{n_{e-1}}),$$

so geht η in die conjugirten Perioden

$$(4) \qquad \eta, \eta_1, \ldots \eta_{e-1}$$

über, und wenn diese alle von einander verschieden sind, so gehört η zur Gruppe $\mathfrak{A}$. Der zu $\mathfrak{A}$ gehörige Körper $\Omega(\eta)$ besteht aus allen rationalen Functionen von η, und die Zahlen $\eta_1 \ldots \eta_{e-1}$ gehören alle zu derselben Gruppe $\mathfrak{A}$.

Wenn aber die Grössen (4) nicht alle von einander verschieden sind, so gehört die Zahl η nicht zu der Gruppe $\mathfrak{A}$, sondern zu einer umfassenderen Gruppe $\mathfrak{A}'$, von der $\mathfrak{A}$ ein Theiler

ist. Um die Bedingungen für diesen Fall zu ermitteln, erweitern wir den Begriff der **Resolventen**, wie wir ihn schon im §. 17 betrachtet haben, noch etwas.

Wir lassen n die Reihe der Zahlen der Gruppe $\mathfrak{N}$ durchlaufen und bezeichnen mit $\chi(n)$ einen der Charaktere dieser Gruppe. Die erweiterten Resolventen sind dann, wenn r eine m^{te} Einheitswurzel ist:

(5) $$(\chi, r) = \sum^{n} \chi(n) r^{n}.$$

Verstehen wir unter $\mathfrak{B}$ die zu $\mathfrak{A}$ reciproke Gruppe und lassen b die Zahlen von $\mathfrak{B}$ durchlaufen, so giebt es nach §. 12, 7. eine dem Grade von $\mathfrak{B}$ gleiche Anzahl von Charakteren χ_b, die dadurch ausgezeichnet sind, dass

$$\chi_b(a) = 1$$

ist, für jede Zahl a aus der Gruppe $\mathfrak{A}$. Daraus folgt dann nach der Definition der Charaktere §. 11, (4) für jedes n:

(6) $$\chi_b(an) = \chi_b(n),$$

d. h. der Charakter χ_b hat für alle Zahlen einer jeden Nebengruppe $\mathfrak{A}n_1, \mathfrak{A}n_2 \ldots$ einen und denselben Werth. Demnach wird die Resolvente (χ_b, r) nur von den Perioden η abhängen, und den Ausdruck erhalten:

(7) $$(\chi_b, r) = \eta + \chi_b(n_1)\eta_1 + \cdots + \chi_b(n_{e-1})\eta_{e-1}.$$

Wenn η zu einer Gruppe $\mathfrak{A}'$ gehört, so gehören die conjugirten Zahlen $\eta_1, \eta_2, \ldots \eta_{e-1}$ zu derselben Gruppe (weil $\mathfrak{A}'$ ein Normaltheiler von $\mathfrak{N}$ ist, Bd. I, §. 154). Wenn also a' irgend eine Zahl aus $\mathfrak{A}'$ ist, so bleiben die Grössen $\eta, \eta_1, \eta_2, \ldots \eta_{e-1}$ durch die Substitution $(r, r^{a'})$ ungeändert und nach (7) ist auch

(8) $$(\chi_b, r) = (\chi_b, r^{a'}).$$

Andererseits erhält man aus (5), wenn man bedenkt, dass $a'n$ zugleich mit n die ganze Gruppe $\mathfrak{N}$ durchläuft,

$$\begin{aligned}(\chi_b, r) &= \sum^{n} \chi_b(na') r^{na'} = \chi_b(a') \sum^{n} \chi_b(n) r^{na'} \\ &= \chi_b(a')(\chi_b, r^{a'}),\end{aligned}$$

also nach (8):

(9) $$(\chi_b, r) = \chi_b(a')(\chi_b, r).$$

Ist $\mathfrak{A}$ nicht mit $\mathfrak{A}'$ identisch, sondern ein echter Theiler von $\mathfrak{A}'$, so ist die zu $\mathfrak{A}'$ reciproke Gruppe $\mathfrak{B}'$ ein echter Theiler von $\mathfrak{B}$ (nach §. 12, 8.); wenn also b eine Zahl in $\mathfrak{B}$ ist, die nicht

zugleich in $\mathfrak{B}'$ enthalten ist, so kann man a' so wählen, dass $\chi_b(a')$ nicht $= 1$ ist. Dann folgt aber aus (9)

(10) $$(\chi_b, r) = 0;$$

also der Satz:

1. Wenn die Periode η nicht zu $\mathfrak{A}$, sondern zu einer umfassenderen Gruppe $\mathfrak{A}'$ gehört, dann verschwindet jede Resolvente (χ_b, r), wenn b eine Zahl aus $\mathfrak{B}$ ist, die nicht in $\mathfrak{B}'$ vorkommt.

Um nun die Bedingungen für diesen Satz weiter zu verfolgen, müssen wir die Bildungsweise der Charaktere berücksichtigen.

Wir wählen die Bezeichnung so, wie wir sie am Schluss des §. 16 eingeführt haben. Dann ist, wenn $\beta_{-1}, \beta_0, \beta_1, \ldots \beta_\mu$ die Indices von b und $\nu_{-1}, \nu_0, \nu_1, \ldots \nu_\mu$ die von n sind,

(11) $$\chi_b(n) = \varepsilon_{-1}^{\beta_{-1}\nu_{-1}} \varepsilon_0^{\beta_0\nu_0} \varepsilon_1^{\beta_1\nu_1} \ldots \varepsilon_\mu^{\beta_\mu\nu_\mu}.$$

Bezeichnen wir mit $r_0, r_1, \ldots r_\mu$ primitive Einheitswurzeln der Grade $2^\lambda, q_1^{\varkappa_1}, q_2^{\varkappa_2}, \ldots q_\mu^{\varkappa_\mu}$, so können wir jede primitive m^{te} Einheitswurzel in der Form darstellen (Bd. I, §. 132)

(12) $$r = r_0 r_1 \ldots r_\mu,$$

und wenn wir $n_0, n_1, \ldots n_\mu$ aus den Congruenzen bestimmen

(13) $$n \equiv n_0 \pmod{2^\lambda},\quad n \equiv n_1 \pmod{q_1^{\varkappa_1}}, \ldots n \equiv n_\mu \pmod{q_\mu^{\varkappa_\mu}},$$

so zerfällt (χ_b, r) nach (5) in das Product der folgenden Summen:

(14) $$\sum^{n_0} \varepsilon_{-1}^{\beta_{-1}\nu_{-1}} \varepsilon_0^{\beta_0\nu_0} r_0^{n_0},\quad \sum^{n_1} \varepsilon_1^{\beta_1\nu_1} r_1^{n_1}, \ldots \sum^{n_\mu} \varepsilon_\mu^{\beta_\mu\nu_\mu} r_\mu^{n_\mu}.$$

Wenn nun b eine Zahl ist, die in $\mathfrak{B}$, aber nicht in $\mathfrak{B}'$ vorkommt, so muss nach dem Satze 1. eine von diesen Summen verschwinden.

Dafür ist aber nach §. 17 die nothwendige und hinreichende Bedingung die, dass eine der Congruenzen

(15) $$\beta_0 \equiv 0 \pmod 2,\quad \beta_1 \equiv 0 \pmod{q_1}, \ldots \beta_\mu \equiv 0 \pmod{q_\mu}$$

befriedigt ist, und zwar eine solche, deren Modul mehrfach in m aufgeht.

Diese Bedingung muss zunächst, wenn die Voraussetzung des Satzes 1. zutrifft, für jede Zahl b, die in $\mathfrak{B}$, aber nicht in $\mathfrak{B}'$ vorkommt, erfüllt sein. Ist aber b' eine Zahl in $\mathfrak{B}'$, so ist für jeden ganzzahligen Exponenten x das Product $b'^x b$ in $\mathfrak{B}$, aber

nicht in $\mathfrak{B}'$ enthalten, und also muss, wenn $\beta_0', \beta_1', \ldots \beta_\mu'$ die Indices von b' sind, für jedes x eine der Congruenzen

$$\begin{aligned} x\beta_0' + \beta_0 &\equiv 0 \pmod{2} \\ x\beta_1' + \beta_1 &\equiv 0 \pmod{q_1} \\ &\cdots\cdots\cdots \\ x\beta_\mu' + \beta_\mu &\equiv 0 \pmod{q_\mu} \end{aligned} \tag{16}$$

befriedigt sein.

Sind nun zwei Zahlen β', β nicht beide durch eine Primzahl q theilbar, so kann man immer über x so verfügen, dass $x\beta' + \beta$ nicht durch q theilbar wird; man braucht nur, wenn β durch q theilbar ist, x durch q nicht theilbar, und wenn β durch q nicht theilbar ist, x durch q theilbar anzunehmen. Man kann also x auch so bestimmen, dass es gleichzeitig mehreren solchen Forderungen genügt. Es folgt also aus (16), dass entweder β_0', β_0 durch 2 oder β_1', β_1 durch $q_1 \ldots$ oder β_μ', β_μ durch q_μ theilbar sein müssen; d. h. eine der Congruenzen (15) muss auch erfüllt sein, wenn b irgend eine Zahl aus $\mathfrak{B}$ ist, gleichviel ob sie in $\mathfrak{B}'$ vorkommt oder nicht. Endlich folgt wieder aus (16), indem wir unter b, b' zwei beliebige Zahlen aus $\mathfrak{B}$ verstehen, dass von den Congruenzen (15) eine und dieselbe für alle Zahlen aus $\mathfrak{B}$ bestehen muss. Dies können wir nun so zusammenfassen:

2. Wenn die Periode η nicht zu $\mathfrak{A}$ gehört, so muss es unter den Primzahlen (einschliesslich 2), die mehr als einmal in m aufgehen, eine geben, q, so dass für jede Zahl b aus $\mathfrak{B}$ der dem q entsprechende Index β durch q theilbar ist.

Wir betrachten jetzt die Gruppe Q, die nach der Bezeichnungsweise (5) des §. 18 durch die Congruenz

$$Q \equiv 1 \left(\text{mod } \frac{m}{q}\right) \tag{17}$$

definirt ist, und bezeichnen mit P die dazu reciproke Gruppe.

Nach dem Satze 7., §. 19 ist jede Gruppe, die wie $\mathfrak{B}$ die Eigenschaft hat, dass der dem q entsprechende Index β durch q theilbar ist, ein Theiler der Gruppe P, und folglich ist nach §. 12, 8. Q ein Theiler von $\mathfrak{A}$, also $\mathfrak{A}$ nach §. 19, 8. ein nicht primärer Theiler von $\mathfrak{N}$, und damit sind wir zu dem Satze gelangt:

3. Ist $\mathfrak{A}$ ein primärer Theiler von $\mathfrak{N}$, so gehört die Periode η zu der Gruppe $\mathfrak{A}$.

Alle primären Theiler des vollen Kreistheilungskörpers Ω_m sind demnach in der Form $\Omega(\eta)$ darstellbar, d. h. alle Zahlen eines solchen Theilers sind rational durch die Kreistheilungsperioden η darstellbar, und da man die nicht primären Theiler von Ω_m als primäre Theiler von niedrigeren Kreistheilungskörpern wiederfindet, so folgt:

4. **Alle Kreistheilungskörper sind in der Form $\Omega(\eta)$ darstellbar.**

Oder auch:

5. **Jede rationale Function von Einheitswurzeln kann als rationale Function einer Kreistheilungsperiode dargestellt werden.**

Und dieser Satz lässt sich auch in der Form aussprechen:

6. **Ist $\mathfrak{A}$ ein beliebiger primärer oder nicht primärer Theiler von $\mathfrak{R}$ vom Index e, so giebt es einen Theiler m_1 von m und eine in Ω_{m_1} gelegene Kreistheilungsperiode η vom Index e, so dass η, als Function von r aufgefasst, eine zur Gruppe $\mathfrak{A}$ gehörige Function ist, also, wenn a zu $\mathfrak{A}$ gehört, durch die Substitution (r, r^a) ungeändert bleibt und für alle Substitutionen von $\mathfrak{R}$ e verschiedene Werthe erhält.**

Durchläuft a eine Gruppe $\mathfrak{A}$, die ein primärer Theiler von $\mathfrak{R}$ ist, und setzen wir

$$\eta_h = \sum^{a} r^{ah},$$

auch wenn h nicht relativ prim zu m ist, so können wir diese Grössen η_h, die alle die Permutationen der Gruppe $\mathfrak{A}$ gestatten, rational durch $\eta = \sum r^a$ darstellen. Andererseits lässt sich aber auch jede rationale Function von η linear durch die η_h darstellen. Dies wird bewiesen sein, wenn gezeigt ist, dass man das Product zweier η_h linear durch die η_h ausdrücken kann. Es ist aber:

$$\eta_h \eta_k = \sum^{a, a'} r^{ha + ka'};$$

nimmt man zuerst die Summe nach a' bei feststehendem a, so kann man a' durch $a a'$ ersetzen, da $a a'$ zugleich mit a' die Gruppe $\mathfrak{A}$ durchläuft. Man erhält so

$$\eta_h \eta_k = \sum^{a, a'} r^{a(h + ka')} = \sum^{a'} \eta_{h + ka'}.$$

Wenn die Primzahl q nur einfach in m aufgeht und $\mathfrak{A}$ durch Q theilbar ist, so ist zwar $\mathfrak{A}$ nicht primär; es gehört aber trotzdem die Periode η zu der Gruppe $\mathfrak{A}$.

Es kann aber in diesem Falle η durch Einheitswurzeln von niedrigerem Grade dargestellt werden. In folgender Weise lässt sich diese Darstellung finden. Alle Zahlen von Q sind von der Form $1 + hm'$, worin h die Reihe der Zahlen $0, 1, \ldots q-1$ durchläuft, mit Ausnahme des einzigen Werthes, für den

$$(18) \qquad 1 + hm' = kq$$

durch q theilbar wird. Setzt man also unter der Voraussetzung, dass $\mathfrak{A}$ durch Q theilbar ist,

$$\mathfrak{A} = Q + Qa_1 + Qa_2 \ldots,$$

so folgt, dass jede Zahl a in $\mathfrak{A}$ von der Form ist:

$$(19) \qquad a = a'(1 + hm'),$$

worin a' die Reihe der Zahlen $1, a_1, a_2 \ldots$ durchläuft. Daraus ist noch zu schliessen, dass die Reste der Zahlen $1, a', a'' \ldots$ nach dem Modul m' eine Gruppe bilden. Nimmt man nun die Summe über alle Werthe $h = 0, 1, \ldots q-1$ und nimmt dann den einen durch (18) bestimmten Werth wieder weg, so folgt:

$$\eta = \sum^{a} r^a = \sum^{a'} \sum^{h} r^{a'(1+hm')} - \sum^{a'} r^{a'kq},$$

oder, da $\sum\limits^{h} r^{a'm'h} = 0$ ist:

$$\eta = -\sum^{a'} r^{a'kq}.$$

Nun ist r^q eine m'^{te} Einheitswurzel, und η also, vom Vorzeichen abgesehen, gleich einer aus m'^{ten} Einheitswurzeln gebildeten Periode [1]).

§. 21.

Kreistheilungskörper mit gegebener Gruppe.

Im Vorhergehenden hat sich also ergeben, dass jede Kreistheilungsperiode

$$\eta = \sum^{a} r^a,$$

in der r eine primitive m^{te} Einheitswurzel ist und a die Zahlen einer Gruppe $\mathfrak{A}$ durchläuft, wenn $\mathfrak{A}$ ein primärer Theiler von $\mathfrak{N}$

[1]) Hier ist die Abhandlung von Fuchs zu vergleichen: Ueber die Perioden, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. Crelle's Journal, Bd. 61 (1863).

ist, die Wurzel einer Abel'schen Gleichung ist, deren Gruppe mit der zu $\mathfrak{A}$ reciproken Gruppe $\mathfrak{B}$ isomorph ist.

Die Aufgabe, die wir jetzt stellen und lösen wollen, ist folgende:

I. **Es soll der Modul m und die Gruppe $\mathfrak{A}$ auf alle mögliche Arten so bestimmt werden, dass $\mathfrak{B}$ ein beliebig gegebenes System von Invarianten hat.**

Oder was dasselbe ist:

Es sollen alle Kreistheilungskörper von gegebener Gruppe bestimmt werden.

Wir machen dabei immer die Voraussetzung, dass $\mathfrak{A}$ ein primärer Theiler von $\mathfrak{R}$ sein soll, weil wir sonst einen und denselben Körper mehrmals erhalten würden. Die Aufgabe zerfällt in zwei Theile, nämlich:

II. **Welche Moduln m sind geeignet, eine Gruppe $\mathfrak{B}$ von gegebenen Invarianten zu erzeugen?**

III. **Wie findet man diese Gruppe $\mathfrak{B}$ und die zugehörige Gruppe $\mathfrak{A}$?**

Wir müssen bei dieser Untersuchung die Bezeichnung gegen das Frühere etwas ändern, damit die Uebersichtlichkeit nicht verloren geht. Die exceptionelle Stellung der Primzahl 2, die bei den bisherigen Betrachtungen immer berücksichtigt werden musste, machte eine etwas umständliche Bezeichnung nothwendig. Diese Unterscheidung ist im Folgenden nicht mehr in dem Maasse nothwendig, und darum lässt sich die Bezeichnung jetzt vereinfachen.

Wir bezeichnen die Indices einer Zahl a aus der Gruppe $\mathfrak{A}$ mit

$$\alpha_1, \alpha_2, \ldots \alpha_\mu \quad \text{(Indices von } a)$$

und die entsprechenden Indexmoduln mit

$$c_1, c_2, \ldots c_\mu \quad \text{(Indexmoduln)},$$

so dass μ gleich der Anzahl der in m aufgehenden Primzahlen, oder wenn m durch 8 theilbar ist, um 1 grösser ist.

Es seien ferner

$$\omega_1, \omega_2, \ldots \omega_\mu$$

primitive Einheitswurzeln der Grade $c_1, c_2, \ldots c_\mu$. Sind nun die Indices einer Zahl b in der zu $\mathfrak{A}$ reciproken Gruppe $\mathfrak{B}$

$$\beta_1, \beta_2, \ldots \beta_\mu \quad \text{(Indices von } b),$$

so ist die Beziehung zwischen den α und den β durch die Gleichung

$$(1) \qquad \omega_1^{\alpha_1 \beta_1} \omega_2^{\alpha_2 \beta_2} \ldots \omega_\mu^{\alpha_\mu \beta_\mu} = 1$$

ausgedrückt.

Die Invarianten der Gruppe $\mathfrak{B}$, die nach §. 10 lauter Primzahlpotenzen sind, wollen wir mit

$$i_1, i_2, \ldots i_\nu \quad \text{(Invarianten von } \mathfrak{B})$$

bezeichnen. Wir nehmen diese Invarianten als beliebig gegebene Primzahlpotenzen an und bezeichnen mit J ihr kleinstes gemeinschaftliches Vielfache, so dass

$$(2) \qquad J = i_1 i_1' = i_2 i_2' = \cdots = i_\nu i_\nu'$$

gesetzt werden kann.

Ausserdem soll $\mathfrak{A}$ als primärer Theiler von $\mathfrak{N}$ vorausgesetzt werden, was nach §. 19, 8. mit der Bedingung gleichbedeutend ist:

IV. Keiner der Indices β soll für alle Zahlen b, wenn die entsprechende Primzahl q mehrmals in m aufgeht, durch q, oder wenn q nur einmal in m aufgeht, durch $q - 1$ theilbar sein.

Nach der Definition der Invarianten muss die Gruppe $\mathfrak{B}$ eine Basis haben, deren Elemente

$$g_1, g_2, \ldots g_\nu \quad \text{(Basis von } \mathfrak{B})$$

von den Graden

$$i_1, i_2, \ldots i_\nu$$

sind, so dass jede Zahl b einmal und nur einmal in der Form

$$(3) \qquad b \equiv g_1^{x_1} g_2^{x_2} \ldots g_\nu^{x_\nu} \pmod{m}$$

enthalten ist, wenn die Exponenten $x_1, x_2, \ldots x_\nu$ je ein volles Restsystem nach den Moduln $i_1, i_2, \ldots i_\nu$ durchlaufen.

Alle Grössen von der Form (3) bilden, wenn $g_1, g_2, \ldots g_\nu$ beliebige Zahlen sind, bei unbeschränkter Veränderlichkeit der ganzzahligen Exponenten x gewiss eine Gruppe. Sollen aber die g_h die Elemente einer Basis dieser Gruppe, und ihre Grade i_h sein, so darf $1 \equiv g_1^{x_1} g_2^{x_2} \ldots g_\nu^{x_\nu} \pmod{m}$ nur dann erfüllt sein, wenn x_h durch i_h theilbar ist, also:

1. Die nothwendige und hinreichende Bedingung dafür, dass $g_1, g_2, \ldots g_\nu$ die Elemente einer Basis einer Gruppe $\mathfrak{B}$ von den Graden $i_1, i_2, \ldots i_\nu$ seien, ist die, dass die Congruenz

$$(4) \qquad g_1^{x_1} g_2^{x_2} \ldots g_\nu^{x_\nu} \equiv 1 \pmod{m}$$

dann und nur dann besteht, wenn zugleich die Congruenzen

(5) $x_1 \equiv 0 \pmod{i_1}$, $x_2 \equiv 0 \pmod{i_2}$, ... $x_\nu \equiv 0 \pmod{i_\nu}$

erfüllt sind.

Hiernach ist also J die kleinste positive Zahl, die für alle b der Congruenz

$$b^J \equiv 1 \pmod{m}$$

genügt, oder die kleinste positive Zahl, für die für alle Systeme der β

(6) $J\beta_1 \equiv 0 \pmod{c_1}$, $J\beta_2 \equiv 0 \pmod{c_2}$, ... $J\beta_\mu \equiv 0 \pmod{c_\mu}$.

Daraus ergeben sich die ersten Schlüsse über die Zusammensetzung der Zahl m.

a) Eine ungerade Primzahl q, die nicht in J enthalten ist, kann nur einfach in m aufgehen.

Denn ist m durch $q^\varkappa$ theilbar, so ist eine der Grössen c, etwa $c_1 = \varphi(q^\varkappa) = q^{\varkappa-1}(q-1)$, also wenn $\varkappa > 1$ ist, so ist c_1 noch durch q theilbar, und aus (6) folgt dann, dass alle β_1 durch q theilbar sein müssten, was der Voraussetzung IV. widerspricht.

b) Eine ungerade Primzahl q, die in J aufgeht, kann höchstens einmal mehr in m, als in J enthalten sein.

Denn man kann ebenso schliessen, dass, wenn $c_1 = q^{\varkappa-1}(q-1)$, und J nicht durch $q^{\varkappa-1}$ theilbar ist, alle β_1 durch q theilbar sein müssten.

c) Ist J ungerade, so muss auch m ungerade sein.

Denn ist m durch eine Potenz von 2, also mindestens durch 4 theilbar, so ist der der Zahl 2 entsprechende Indexmodul gerade, und die entsprechenden β müssten nach (6) alle gerade sein, entgegen der Forderung IV.

d) Ist J durch eine Potenz von 2 theilbar, so kann m den Factor 2 höchstens zweimal öfter enthalten, als J.

Denn ist m durch 2^λ theilbar und $\lambda > 2$, so sind zwei der Indexmoduln

$$c_1 = 2, \quad c_2 = 2^{\lambda-2}.$$

Wäre also J nicht durch $2^{\lambda-2}$ theilbar, so müssten alle β_2 durch 2 theilbar sein, was wieder gegen die Forderung IV ist.

e) Wenn q eine einfach in m aufgehende Primzahl ist, so muss $q - 1$ wenigstens durch eine der in J aufgehenden Primzahlen theilbar sein.

Denn wäre $c_1 = q - 1$ relativ prim zu J, so müssten alle β_1 durch $q - 1$ theilbar sein, im Widerspruch mit IV. Die weiteren Bedingungen für m ergeben sich später.

Bestimmung der Gruppe $\mathfrak{B}$:

Die Gruppe $\mathfrak{B}$ ist bestimmt, wenn ihre Basis $g_1, g_2, \ldots g_\nu$ gegeben ist. Die Elemente der Basis wollen wir durch ihre Indices bestimmen, und führen also folgende Bezeichnung ein. Es seien

(7)
$$\begin{array}{llll} \gamma_{1,1}, \gamma_{1,2}, \ldots \gamma_{1,\mu} & \text{die Indices von} & g_1 \\ \gamma_{2,1}, \gamma_{2,2}, \ldots \gamma_{2,\mu} & \text{"} \quad \text{"} \quad \text{"} & g_2 \\ \ldots\ldots\ldots & & \\ \gamma_{\nu,1}, \gamma_{\nu,2}, \ldots \gamma_{\nu,\mu} & \text{"} \quad \text{"} \quad \text{"} & g_\nu. \end{array}$$

Die Indices $\beta_1, \beta_2, \ldots \beta_\mu$ eines beliebigen Elementes b erhält man dann nach (3) in der Form:

(8)
$$\begin{aligned} \beta_1 &\equiv \gamma_{1,1}\, x_1 + \gamma_{2,1}\, x_2 + \cdots + \gamma_{\nu,1}\, x_\nu \pmod{c_1} \\ \beta_2 &\equiv \gamma_{1,2}\, x_1 + \gamma_{2,2}\, x_2 + \cdots + \gamma_{\nu,2}\, x_\nu \pmod{c_2} \\ &\ldots\ldots\ldots \\ \beta_\mu &\equiv \gamma_{1,\mu}\, x_1 + \gamma_{2,\mu}\, x_2 + \cdots + \gamma_{\nu,\mu}\, x_\nu \pmod{c_\mu}, \end{aligned}$$

und wir fragen nun nach den nothwendigen und hinreichenden Bedingungen für die Zahlen $\gamma_{h,k}$, damit $g_1, g_2 \ldots g_\nu$ die Basis einer Gruppe $\mathfrak{B}$ von den verlangten Eigenschaften ist. Nach 1. ist hierfür zuerst nothwendig:

2. Die Zahlen $\gamma_{h,k}$ müssen so beschaffen sein, dass die Congruenzen

(9)
$$\begin{aligned} &\gamma_{1,1}\, x_1 + \gamma_{2,1}\, x_2 + \cdots + \gamma_{\nu,1}\, x_\nu \equiv 0 \pmod{c_1} \\ &\gamma_{1,2}\, x_1 + \gamma_{2,2}\, x_2 + \cdots + \gamma_{\nu,2}\, x_\nu \equiv 0 \pmod{c_2} \\ &\ldots\ldots\ldots \\ &\gamma_{1,\mu}\, x_1 + \gamma_{2,\mu}\, x_2 + \cdots + \gamma_{\nu,\mu}\, x_\nu \equiv 0 \pmod{c_\mu} \end{aligned}$$

dann und nur dann erfüllt sind, wenn zugleich die Congruenzen

(10) $x_1 \equiv 0 \pmod{i_1}$, $x_2 \equiv 0 \pmod{i_2}$, ... $x_\nu \equiv 0 \pmod{i_\nu}$

bestehen.

Ist diese Bedingung erfüllt, so ist gewiss $g_1, g_2, \ldots g_\nu$ die Basis einer Gruppe mit den Invarianten $i_1, i_2, \ldots i_\nu$. Wenn aber auch noch die in IV. aufgestellte Forderung erfüllt sein soll, dann folgt noch weiter:

3. Ist q_h eine in m aufgehende Primzahl, der der Index β_h entspricht, so dürfen die ν Grössen

$$\gamma_{1,h}, \gamma_{2,h}, \ldots \gamma_{\nu,h},$$

wenn q_h mehrfach in m aufgeht, nicht alle durch q_h, und wenn q_h nur einmal in m aufgeht, nicht alle durch $q_h - 1$ theilbar sein.

Die Bedingungen 2., 3. sind dann also die nothwendigen und hinreichenden, und es kommt jetzt nur noch darauf an, sie in eine Form zu bringen, dass die Möglichkeit ihrer Erfüllung beurtheilt werden kann.

Wir bezeichnen mit

$\delta_{k,h}$ den grössten gemeinschaftlichen Theiler von i_k und c_h und setzen

$$(11) \qquad i_k = \delta_{k,h}\, i_{k,h}, \quad c_h = \delta_{k,h}\, c_{k,h}, \quad \begin{matrix} k = 1, 2, \ldots \nu, \\ h = 1, 2, \ldots \mu, \end{matrix}$$

so dass $i_{k,h}$ und $c_{k,h}$ relativ prim sind. Es ist dann zu bemerken, dass die Grössen

$$\delta_{k,h}, \quad i_{k,h}, \quad c_{k,h}$$

durch m und die Invarianten i_k völlig bestimmt sind. Nach der Definition der Invarianten müssen die $\delta_{k,h}$ und $i_{k,h}$ Primzahlpotenzen sein.

Aus den Voraussetzungen, die wir in a) bis d) über die Zahl m gemacht haben, ergiebt sich eine Folgerung für die $c_{k,h}$, die wir hervorheben müssen.

4. Ist $q_h^\varkappa$ einer der Factoren von m, der dem Index β_h entspricht, ist also $c_h = q_h^{\varkappa-1}(q_h - 1)$, oder wenn $q = 2$ und $\varkappa > 2$ ist, $c_h = 2^{\varkappa-2}$, und wenn $\varkappa = 2$ ist, $c_h = 2$, so können, wenn $\varkappa > 1$ ist, die Zahlen

$$(12) \qquad c_{1,h}, c_{2,h}, \ldots c_{\nu,h}$$

nicht alle durch q_h, und wenn $\varkappa = 1$ ist, nicht alle durch $q - 1$ theilbar sein.

Wenn nämlich die Grössen (12) alle durch q_h theilbar sind, so sind nach (11) die Zahlen

$$(13) \qquad \delta_{1,h}, \delta_{2,h}, \ldots \delta_{\nu,h}$$

alle nicht durch $q_h^{\varkappa-1}$ theilbar, und die Zahlen

(14) $$i_{1,h},\ i_{2,h},\ \ldots\ i_{\nu,h}$$

sind alle nicht durch q_h theilbar, folglich ist nach (11) keine der Zahlen $i_1, i_2, \ldots i_\nu$, und also auch J nicht durch $q_h^{\varkappa-1}$ theilbar, was den Annahmen a) und b) widerspricht. Für $q_h = 2$ ist in diesem Schlusse nur $\varkappa - 1$ oder 2 (bei $\varkappa = 2$) an Stelle von $\varkappa$ zu setzen, um denselben Widerspruch gegen c) und d) zu erhalten.

Ist aber $\varkappa = 1$ und sind die Zahlen (12) alle durch $q_h - 1$ theilbar, so müssen sie gleich $q_h - 1$ sein; die Zahlen (13) sind alle $= 1$ und es würde also folgen, dass die Zahlen i_k und also auch J relativ prim zu $q_h - 1$ wären, was der Voraussetzung e) widerspricht.

Wenn wir jetzt zu der in 2. ausgesprochenen Forderung für die Grössen $\gamma_{k,h}$ zurückkehren, so ergiebt sich zunächst, dass die Congruenzen (9) erfüllt sein müssen, wenn $x_k = i_k$ und die übrigen $x = 0$ gesetzt werden, also:

$$\gamma_{k,h}\, i_k \equiv 0 \pmod{c_h},$$

und daraus mit Berücksichtigung von (11):

$$i_{k,h}\, \gamma_{k,h} \equiv 0 \pmod{c_{k,h}}.$$

Weil aber $i_{k,h}$ und $c_{k,h}$ relativ prim sind, so folgt, dass $\gamma_{k,h}$ durch $c_{k,h}$ theilbar sein muss. Wir führen also ein neues System von ganzen Zahlen $e_{k,h}$ ein durch die Gleichungen

(15) $$\gamma_{k,h} = c_{k,h}\, e_{k,h}$$

und suchen nun für diese Zahlen die aus 2. folgenden Bedingungen. Da die Zahlen $\gamma_{k,h}$, wie aus ihrer Definition hervorgeht, nur nach dem Modul c_h bestimmt sind, so ist $e_{k,h}$ nur nach dem Modul $\delta_{k,h}$ zu bestimmen. Nehmen wir eine von den Congruenzen (9):

$$\gamma_{1,h}\, x_1 + \gamma_{2,h}\, x_2 + \cdots + \gamma_{\nu,h}\, x_\nu \equiv 0 \pmod{c_h},$$

und führen darin (15) ein, so erhält sie die Form

(16) $$c_{1,h} e_{1,h} x_1 + c_{2,h} e_{2,h} x_2 + \cdots + c_{\nu,h} e_{\nu,h} x_\nu \equiv 0 \pmod{c_h}.$$

Hierin setzen wir nun nach (11):

$$c_{k,h} = \frac{c_h}{\delta_{k,h}} = \frac{c_h\, i_{k,h}}{i_k}.$$

Demnach sind die Congruenzen (16) gleichbedeutend mit der Forderung, dass

$$\frac{e_{1,h}\, i_{1,h}\, x_1}{i_1} + \frac{e_{2,h}\, i_{2,h}\, x_2}{i_2} + \cdots \frac{e_{\nu,h}\, i_{\nu,h}\, x_\nu}{i_\nu}$$

ganze Zahlen sein müssen, oder, mit Rücksicht auf die Bezeichnung (2), mit den Congruenzen:

$$(17) \qquad e_{1,h}\, i_{1,h}\, i'_1 x_1 + e_{2,h}\, i_{2,h}\, i'_2 x_2 + \cdots e_{\nu,h}\, i_{\nu,h}\, i'_\nu x_\nu \equiv 0 \pmod{J}.$$

Diese Congruenzen sind, wie man sieht, immer erfüllt, wenn x_1 durch i_1, x_2 durch $i_2 \ldots$, x_ν durch i_ν theilbar ist, und die Forderung 2. reducirt sich also jetzt darauf:

5. dass die $e_{k,h}$ so zu bestimmen sind, dass die Congruenzen (17) für keine anderen als den Congruenzen $x_k \equiv 0 \pmod{i_k}$ genügende Werthe der x befriedigt sein sollen.

Dazu kommt noch als Umformung der Forderung 3.:

6. Die Zahlen

$$c_{1,h}\, e_{1,h},\quad c_{2,h}\, e_{2,h}, \ldots\ c_{\nu,h}\, e_{\nu,h}$$

dürfen nicht alle durch q_h, wenn $\varkappa > 1$, und durch $(q_h - 1)$, wenn $\varkappa = 1$ ist, theilbar sein.

Die Forderung 6. enthält wegen 4. keine Unmöglichkeit.

Durch 5. und 6. sind die nothwendigen und hinreichenden Bedingungen für die Zahlen $e_{h,k}$ ausgedrückt.

Es handelt sich also jetzt noch um die Frage, ob und unter welchen Voraussetzungen diese Forderungen durch geeignete Wahl der $e_{h,k}$ befriedigt werden können.

Diese Frage wird dadurch sehr vereinfacht, dass sich die Congruenz (17) in mehrere spalten lässt. Die Invarianten i_k sind, wie wir angenommen haben, Primzahlpotenzen. Es möge eine von diesen Primzahlen mit p bezeichnet sein, und es sei

$$(18) \qquad i_1 = p^{\pi_1},\ i_2 = p^{\pi_2}, \ldots\ i_\varrho = p^{\pi_\varrho},$$

während die übrigen i_k, wenn noch solche vorhanden sind, nicht mehr durch p theilbar sein sollen. Den grössten der Exponenten $\pi_1, \pi_2, \ldots \pi_\varrho$ wollen wir mit π bezeichnen.

Dann ist

$$J = p^\pi J',$$

und J' ist nicht mehr durch p theilbar. Es ist ferner

$$i'_1 = p^{\pi-\pi_1} J',\ i'_2 = p^{\pi-\pi_2} J', \ldots\ i'_\varrho = p^{\pi-\pi_\varrho} J',$$

während $i'_{\varrho+1}, \ldots i'_\nu$ durch p^π theilbar sind.

Demnach hat die Congruenz (17) zur Folge:

$$(19)\quad e_{1,h}\, i_{1,h}\, p^{\pi-\pi_1} x_1 + e_{2,h}\, i_{2,h}\, p^{\pi-\pi_2} x_2 + \cdots e_{\varrho,h}\, i_{\varrho,h}\, p^{\pi-\pi_\varrho} x_\varrho \equiv 0 \pmod{p^\pi} \qquad h = 1, 2, \ldots \mu,$$

und die übrigen in J aufgehenden Primzahlen ergeben jede ein eben solches System von Congruenzen, die in ihrer Gesammtheit vollständig gleichbedeutend mit der Congruenz (17) sind. Diese Congruenzen (19) dürfen nicht anders befriedigt werden können, als dadurch, dass die Zahlen

$$p^{\pi-\pi_1} x_1, \quad p^{\pi-\pi_2} x_2, \ \ldots \ p^{\pi-\pi_\varrho} x_\varrho$$

durch p^π theilbar sind.

Setzen wir also zur Abkürzung:

$$p^{\pi-\pi_1} x_1 = y_1, \quad p^{\pi-\pi_2} x_2 = y_2, \ \ldots \ p^{\pi-\pi_\varrho} x_\varrho = y_\varrho,$$

so erhält (19) die Form:

$$(20)\quad e_{1,h}\, i_{1,h}\, y_1 + e_{2,h}\, i_{2,h}\, y_2 + \cdots e_{\varrho,h}\, i_{\varrho,h}\, y_\varrho \equiv 0 \pmod{p^\pi},$$

und diese Congruenzen sollen

$$y_1 \equiv 0, \quad y_2 \equiv 0, \ \ldots \ y_\varrho \equiv 0 \pmod{p^\pi}$$

zur nothwendigen Folge haben.

Das System von linearen Congruenzen (20) kann nun mit denselben Mitteln discutirt werden, wie ein System linearer Gleichungen, nämlich durch die Determinanten (vgl. den Abschnitt II des ersten Bandes).

Wir wollen zur besseren Uebersicht die Congruenzen (20) für den Augenblick so schreiben:

$$(21)\quad \begin{array}{l} a_{1,1}\, y_1 + a_{2,1}\, y_2 + \cdots + a_{\varrho,1}\, y_\varrho \equiv 0 \\ a_{1,2}\, y_1 + a_{2,2}\, y_2 + \cdots + a_{\varrho,2}\, y_\varrho \equiv 0 \\ \cdots\cdots\cdots\cdots\cdots \\ a_{1,\mu}\, y_1 + a_{2,\mu}\, y_2 + \cdots + a_{\varrho,\mu}\, y_\varrho \equiv 0 \end{array} \pmod{p^\pi}.$$

Wenn die Coëfficienten $a_{k,h}$ alle durch p theilbar sind, dann sind diese Congruenzen schon befriedigt, wenn die y alle nur durch $p^{\pi-1}$ theilbar sind, und dieser Fall darf also nicht eintreten.

Wir wollen nun annehmen, es lasse sich aus der Matrix

$$(22)\quad \begin{array}{l} a_{1,1},\ a_{2,1},\ \ldots\ a_{\varrho,1} \\ a_{1,2},\ a_{2,2},\ \ldots\ a_{\varrho,2} \\ \cdots\cdots\cdots \\ a_{1,\mu},\ a_{2,\mu},\ \ldots\ a_{\varrho,\mu} \end{array}$$

eine Determinante von τ Reihen bilden, die nicht durch p theilbar ist, während alle Determinanten von mehr als τ Reihen, wenn solche vorhanden sind, durch p theilbar sind. Wir können voraussetzen, dass die Indices so angeordnet sind, dass

$$\varDelta = \Sigma \pm a_{1,1}\, a_{2,2} \ldots a_{\tau,\tau}$$

nicht durch p theilbar ist. Bezeichnen wir mit $\varDelta_{k,h}$ die Unterdeterminanten von $\varDelta$ und setzen

$$\varDelta_{k,1}\, a_{s,1} + \varDelta_{k,2}\, a_{s,2} + \cdots \varDelta_{k,\tau}\, a_{s,\tau} = D_{k,s},$$

so ist $D_{k,s} = \varDelta$, wenn $k = s$, und $= 0$, wenn $s \gtreqless \tau$ und von k verschieden ist, und ist, wenn $s > \tau$ ist, eine τ-reihige Determinante der Matrix (22). Mit Hülfe dieser Bezeichnung lassen sich nun aus den τ ersten Congruenzen (21) die folgenden herleiten:

$$(23)\qquad \begin{array}{l} \varDelta y_1 + D_{1,\tau+1}\, y_{\tau+1} + \cdots D_{1,\varrho}\, y_\varrho \equiv 0 \\ \varDelta y_2 + D_{2,\tau+1}\, y_{\tau+1} + \cdots D_{2,\varrho}\, y_\varrho \equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \varDelta y_\tau + D_{\tau,\tau+1}\, y_{\tau+1} + \cdots D_{\tau,\varrho}\, y_\varrho \equiv 0. \end{array} \pmod{p^\pi}$$

Setzen wir zur Abkürzung

$$A_{s,r} = \varDelta\, a_{s,r} - \sum_{1,\tau}^{k} a_{k,r}\, D_{k,s} = \varDelta\, a_{s,r} - \sum_{1,\tau}^{h} \sum_{1,\tau}^{k} \varDelta_{k,h}\, a_{s,h}\, a_{k,r},$$

so ist $A_{s,r}$ nach Bd. I, §. 23 eine $(\tau + 1)$-reihige Determinante der Matrix (22) und also nach Voraussetzung durch p theilbar.

Nach dieser Bezeichnungsweise erhalten wir aus (23):

$$\begin{array}{l} \varDelta\,(a_{1,r}\, y_1 + a_{2,r}\, y_2 + \cdots + a_{\varrho,r}\, y_\varrho) \\ \equiv A_{\tau+1,r}\, y_{\tau+1} + \cdots + A_{\varrho,r}\, y_\varrho \pmod{p^\pi}, \end{array}$$

und es zeigt sich also, dass, wenn $\tau < \varrho$ ist, die Congruenzen (20) schon befriedigt sind, wenn $y_{\tau+1}, \ldots y_\varrho$ durch $p^{\pi-1}$ theilbar angenommen werden, weil alle $A_{s,r}$ durch p theilbar sind. Dies ist also nicht zulässig. Es muss also $\tau = \varrho$ sein, und dies genügt auch, weil dann (23) sich auf

$$\varDelta y_1 \equiv 0, \quad \varDelta y_2 \equiv 0 \ldots \varDelta y_\varrho \equiv 0 \pmod{p^\pi}$$

reducirt, und folglich, da $\varDelta$ durch p nicht theilbar ist, $y_1, y_2, \ldots y_\varrho$ durch p^π theilbar sein müssen.

Hierdurch ist die Forderung 6. in eine andere Form gebracht, die wir, indem wir zu unserer ursprünglichen Bezeichnung in (20) zurückkehren, so aussprechen können:

7. **Es muss die Anzahl ϱ der durch eine Primzahl p theilbaren Invarianten gleich oder kleiner als die Anzahl μ der Indexmoduln sein, und es muss sich aus der Matrix**

$$(24)\qquad \begin{matrix} e_{1,1}\, \dot{i}_{1,1}, & e_{2,1}\, \dot{i}_{2,1}, & \ldots & e_{\varrho,1}\, \dot{i}_{\varrho,1} \\ e_{1,2}\, \dot{i}_{1,2}, & e_{2,2}\, \dot{i}_{2,2}, & \ldots & e_{\varrho,2}\, \dot{i}_{\varrho,2} \\ \cdot & \cdot & \cdot & \cdot \\ e_{1,\mu}\, \dot{i}_{1,\mu}, & e_{2,\mu}\, \dot{i}_{2,\mu}, & \ldots & e_{\varrho,\mu}\, \dot{i}_{\varrho,\mu} \end{matrix}$$

wenigstens eine durch p untheilbare Determinante von ϱ Reihen bilden lassen.

Dies involvirt zunächst eine Forderung für die $i_{k,h}$, d. h. also in letzter Instanz eine Bedingung für die Zahl m.

Alle Glieder irgend einer ϱ-reihigen Determinante der Matrix (24) enthalten einen Factor der Form

$$\dot{i}_{1,h_1}\, \dot{i}_{2,h_2}, \ldots \dot{i}_{\varrho,h_\varrho},$$

worin $h_1, h_2, \ldots h_\varrho$ irgend eine Combination von ϱ verschiedenen Zahlen der Reihe $1, 2, \ldots \mu$ bedeuten. Wären nun alle diese Producte durch p theilbar, so wären sicher alle Determinanten der Matrix (24) von ϱ Reihen auch durch p theilbar, und es muss also wenigstens eine solche Combination geben, die nicht durch p theilbar ist. Weil aber die $i_{k,h}$ nur Potenzen von p sein können, so muss

$$i_{1,h_1} = 1, \quad i_{2,h_2} = 1, \ldots i_{\varrho,h_\varrho} = 1$$

sein. Geht man nun auf die Bedeutung der $i_{k,h}$ in (11) zurück, so können wir die letzte Forderung für den Grad m folgendermaassen ausdrücken:

f) **Wenn eine Primzahl p in ϱ Invarianten $i_1, i_2, \ldots i_\varrho$ aufgeht, so muss die Anzahl μ der Indexmoduln gleich oder grösser als ϱ sein, und es müssen sich ϱ dieser Indexmoduln $c_{h_1}, c_{h_2}, \ldots c_{h_\varrho}$ so auswählen lassen, dass c_{h_1} durch i_1, c_{h_2} durch $i_2 \ldots$, c_{h_ϱ} durch i_ϱ theilbar ist**[1].

[1]) Der Nachweis der Thatsache, dass dieser Forderung immer auf unendlich viele Arten entsprochen werden kann, stützt sich auf den Satz der Zahlentheorie, dass unter den Zahlen einer arithmetischen Progression, deren Anfangsglied und Differenz ohne gemeinsamen Theiler sind, unendlich viele Primzahlen vorkommen, ein Satz, der bis jetzt nur von

Hiermit aber ist alles erschöpft, was wir von m fordern müssen. Denn wenn diese Bedingung f) befriedigt ist, so brauchen wir z. B. nur die $e_{1,h_1}, e_{2,h_2}, \ldots e_{\varrho,h_\varrho}$ durch p untheilbar, die übrigen e durch p theilbar anzunehmen; dann ist die Determinante

$$\begin{vmatrix} e_{1,h_1}\, i_{1,h_1}, & \ldots & e_{1,h_\varrho}\, i_{1,h_\varrho} \\ \cdot & \cdot & \cdot \\ e_{\varrho,h_1}\, i_{\varrho,h_1}, & \ldots & e_{\varrho,h_\varrho}\, i_{\varrho,h_\varrho} \end{vmatrix} \equiv e_{1,h_1}\, e_{2,h_2} \ldots e_{\varrho,h_\varrho} \pmod p$$

also sicher durch p untheilbar.

Und bei dieser Annahme kann auch noch die Bedingung 6. befriedigt werden. Um dies einzusehen, bezeichne man mit p^π irgend eine der Invarianten, etwa i_1, und mit c_h den Indexmodul, der nach f) durch p^π theilbar ist, so dass

(25) $$c_h = p^\pi\, c_{1,h}$$

ist. Ist dann q_h der zum Indexmodul c_h gehörige Primtheiler von m, so ist p entweder gleich q_h oder ein Theiler von $q_h - 1$. Nach der zuletzt gemachten Annahme ist $e_{1,h}$ nicht durch p theilbar, während $e_{2,h}, e_{3,h}, \ldots e_{\nu,h}$ durch p theilbar sind. Es sollen dann die Producte

$$c_{1,h}\, e_{1,h}, \quad c_{2,h}\, e_{2,h}, \ldots c_{\nu,h}\, e_{\nu,h}$$

nicht alle durch q_h oder durch $q_h - 1$ theilbar sein.

Ist zunächst q_h ein einfacher Theiler von m, so ist $c_h = q_h - 1$, und wegen (25) ist $c_{1,h}$ nicht durch $q_h - 1$ theilbar. Man kann also $e_{1,h}$ noch so annehmen, dass $c_{1,h}\, e_{1,h}$ nicht durch $q_h - 1$ theilbar ist. Ist aber q_h ein $\varkappa$-facher Theiler von m und $\varkappa > 1$, und ist $q_h = p$, so ist, wenn p ungerade ist, $c_h = p^{\varkappa-1}(p-1)$, und nach der Voraussetzung b) $\pi \gtreqless \varkappa - 1$. Wenn also c_h durch p^π theilbar sein soll, so muss $\pi = \varkappa - 1$ sein, und (25) ergiebt $c_{1,h} = p - 1$. Ist aber $p = 2$, so ist $c_h = 2$ oder $= 2^{\varkappa-1}$, und es muss also nach der Voraussetzung d) $\pi = 1$ oder $= \varkappa - 2$ sein, und es ist $c_{1,h} = 1$. Man kann also

---

Dirichlet mit Anwendung der Integralrechnung bewiesen ist. (Abhandlungen der Berliner Akademie 1837; Dirichlet's Werke, Bd. I, Nr. 21; Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, Supplement VI; Bachmann, Analytische Zahlentheorie, Abschn. IV). Behalten wir die oben benutzte Bezeichnung bei, so kann man, um für ein gegebenes p der Forderung f) zu genügen, $p^{\pi+1}$ als Factor in m aufnehmen. Dann aber müssen, wenn $\varrho > 1$ ist, noch $\varrho - 1$ Primfactoren q in m vorkommen, die an Congruenzen von der Form $q \equiv 1 \pmod{i_1} \ldots$ gebunden sind.

auch in diesen Fällen $e_{1,h}$ so annehmen, dass $c_{1,h}\,e_{1,h}$ durch q_h nicht theilbar wird.

Die Forderungen, die hiermit für die $e_{k,h}$ gestellt sind, bestehen also nur darin, dass sie durch gewisse Primzahlen theilbar, durch andere nicht theilbar sein sollen, und sind also noch auf unendlich viele Arten mit einander verträglich. Aber diese letzte Annahme über die $e_{k,h}$ hatte nur den Zweck, zu zeigen, dass die früheren allgemeineren Forderungen immer befriedigt werden können. Es kann noch viele andere Arten geben, ihnen zu genügen.

Uebersicht der Resultate.

Wenn es sich darum handelt, alle Kreistheilungskörper, und jeden nur einmal, und zwar auf möglichst einfache Art, durch Kreistheilungsperioden darzustellen, so verfahre man so:

Man nehme ein beliebiges System von Primzahlpotenzen als Invarianten

$$i_1, i_2, \ldots i_\nu$$

an, und wähle dann eine Zahl m nach folgenden Bedingungen.

Wenn p^π die höchste Potenz einer Primzahl p ist, die unter den Invarianten vorkommt, so nehme man p höchstens $(\pi + 1)$-, oder, wenn $p = 2$ ist, $(\pi + 2)$ mal in m auf.

Eine Primzahl q, die gar nicht in den Invarianten aufgeht, darf nur einfach in m aufgenommen werden; aber nur solche einfache Primfactoren q darf m haben, bei denen $q - 1$ durch einen der Primfactoren p der Invarianten theilbar ist. Also kann auch p selbst nur dann einfach in m vorkommen, wenn $p - 1$ durch eines der anderen p theilbar ist.

Ferner muss m noch der Bedingung genügen, dass unter den Indexmoduln

$$c_1, c_2, \ldots c_\mu$$

ϱ verschiedene, wie $c_1, c_2, \ldots c_\varrho$, durch $i_1, i_2, \ldots i_\varrho$ theilbar sind, wenn $i_1, i_2, \ldots i_\varrho$ Potenzen von einer und derselben Primzahl sind. Dann bestimme man die Grössen $i_{k,h}$ und $c_{k,h}$ nach den Formeln (11) und theile die gegebenen Invarianten in Systeme ein, so dass alle Potenzen einer und derselben Primzahl in einem Systeme vereinigt sind.

Für jedes dieser Systeme bilde man die Matrix (24) und wähle die Zahlen $c_{k,h}$ so, dass aus jeder solchen Matrix eine

Determinante von ϱ Reihen gebildet werden kann, die durch die betreffende Primzahl nicht theilbar ist, und dass nicht alle Producte

$$c_{1,h}\, e_{1,h},\; c_{2,h}\, e_{2,h},\; \ldots\; c_{\nu,h}\, e_{\nu,h}$$

durch q_h oder durch $q_h - 1$ theilbar werden. Dann setze man

$$\gamma_{k,h} = c_{k,h}\, e_{k,h},$$

und hat so nach (7) die Indices einer Basis einer Abel'schen Gruppe $\mathfrak{B}$, deren reciproke Gruppe $\mathfrak{A}$ ein primärer Theiler der ganzen Gruppe $\mathfrak{R}$ ist.

§. 22.

Bestimmung der Gruppe $\mathfrak{A}$.

Das letzte Ziel dieser Untersuchung ist nicht sowohl die Bestimmung der Gruppe $\mathfrak{B}$, als die der Gruppe $\mathfrak{A}$, aus der man direct die Kreistheilungsperioden $\eta = \sum r^a$ bilden kann. Diese Aufgabe kann man auf folgende Art lösen: Nach (1) sind die Indices α der Zahlen in $\mathfrak{A}$ von den β abhängig durch die Gleichung

(1) $$\omega_1^{\alpha_1 \beta_1}\, \omega_2^{\alpha_2 \beta_2} \ldots \omega_\mu^{\alpha_\mu \beta_\mu} = 1,$$

worin $\omega_1, \omega_2, \ldots \omega_\mu$ feste primitive Einheitswurzeln der Grade $c_1, c_2, \ldots c_\mu$ bedeuten. Versteht man aber unter C das kleinste gemeinschaftliche Vielfache von $c_1, c_2, \ldots c_\mu$ und setzt

(2) $$C = c_1 c_1' = c_2 c_2' = \cdots = c_\mu c_\mu',$$

und bezeichnet mit ω eine primitive Cte Einheitswurzel, so kann man statt (1) auch setzen

$$\omega^{c_1' \alpha_1 \beta_1 + c_2' \alpha_2 \beta_2 + \cdots + c_\mu' \alpha_\mu \beta_\mu} = 1,$$

und bekommt daher für die α die Congruenz

$$c_1' \alpha_1 \beta_1 + c_2' \alpha_2 \beta_2 + \cdots + c_\mu' \alpha_\mu \beta_\mu \equiv 0 \pmod{C},$$

die gleichbedeutend ist mit der Bedingung, dass die Summen

$$\frac{\alpha_1 \beta_1}{c_1} + \frac{\alpha_2 \beta_2}{c_2} + \cdots + \frac{\alpha_\mu \beta_\mu}{c_\mu} = \sum_{1,\mu}^{h} \frac{\alpha_h \beta_h}{c_h}$$

ganze Zahlen sein müssen. Wenn man darin für β_k die Ausdrücke §. 21, (8) substituirt, so folgt, dass auch

$$\sum^{k} x_k \sum^{h} \frac{\alpha_h\, \gamma_{k.h}}{c_h},$$

oder, da die ganzen Zahlen x_k beliebig sind, die Summen

$$\sum_{1,\mu}^{h} \frac{\alpha_h \gamma_{k,h}}{c_h} \qquad k = 1, 2, \ldots \nu$$

ganze Zahlen sein müssen. Setzt man dann nach (15) und (11) §. 21

$$\gamma_{k,h} = c_{k,h}\, e_{k,h}, \quad c_h = \delta_{k,h}\, c_{k,h}, \quad \dot{\imath}_k = \delta_{k,h}\, \dot{\imath}_{k,h},$$

so folgt, dass

$$\sum^{h} \frac{\alpha_h e_{k,h}}{\delta_{k,h}} = \sum^{h} \frac{\alpha_h \dot{\imath}_{k,h} e_{k,h}}{\dot{\imath}_k}$$

ganze Zahlen sein müssen, und diese Forderung ist gleichbedeutend mit dem System der Congruenzen

$$\sum^{h} \alpha_h\, \dot{\imath}_{k,h}\, e_{k,h} \equiv 0 \pmod{\dot{\imath}_k},$$

oder, ausführlicher geschrieben

$$(3)\quad \begin{array}{l} e_{1,1}\dot{\imath}_{1,1}\alpha_1 + e_{1,2}\dot{\imath}_{1,2}\alpha_2 + \cdots + e_{1,\mu}\dot{\imath}_{1,\mu}\alpha_\mu \equiv 0 \pmod{\dot{\imath}_1} \\ e_{2,1}\dot{\imath}_{2,1}\alpha_1 + e_{2,2}\dot{\imath}_{2,2}\alpha_2 + \cdots + e_{2,\mu}\dot{\imath}_{2,\mu}\alpha_\mu \equiv 0 \pmod{\dot{\imath}_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ e_{\nu,1}\dot{\imath}_{\nu,1}\alpha_1 + e_{\nu,2}\dot{\imath}_{\nu,2}\alpha_2 + \cdots + e_{\nu,\mu}\dot{\imath}_{\nu,\mu}\alpha_\mu \equiv 0 \pmod{\dot{\imath}_\mu}. \end{array}$$

Durch diese Congruenzen sind, wie es sein muss, die Zahlen $\alpha_1, \alpha_2, \ldots \alpha_\mu$ nur nach den Moduln $c_1, c_2, \ldots c_\mu$ bestimmt, weil $\dot{\imath}_{k,h}\, c_h = \dot{\imath}_k\, c_{k,h}$ durch $\dot{\imath}_k$ theilbar ist, und um die Indices aller Zahlen der Gruppe $\mathfrak{A}$ zu finden, hat man einfach alle Lösungen der Congruenzen (3) aufzusuchen.

Vierter Abschnitt.

Cubische und biquadratische Abel'sche Körper.

---

§. 23.

Cubische Kreistheilungskörper.

Die allgemeinen Untersuchungen, die in den letzten Paragraphen dargestellt sind, gestatten mannigfache Anwendungen auf specielle Fälle, von denen die einfachsten hier betrachtet werden sollen. Es ist dabei bemerkenswerth, dass schon die einfachsten Fälle, wenn man sie direct angreift, fast in dieselben Schwierigkeiten hineinführen, die wir durch die allgemeine Untersuchung überwunden haben.

Wir wollen zuerst die Aufgabe behandeln, alle cubischen Kreistheilungskörper, also alle Kreistheilungsperioden, die einer rationalen Gleichung 3ten Grades genügen, aufzufinden, und zwar so, dass von mehreren Ausdrücken, deren dieselbe Grösse fähig ist, der einfachste gesetzt wird.

Wir haben hier nur eine Invariante $i_1 = 3$, und nach den Vorschriften in der Zusammenstellung des §. 21 dürfen in m aufgenommen werden der Factor 9, nicht aber 3, ferner Primzahlen in beliebiger Menge von der Form $6N + 1$, also die Primzahlen 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97 . . ., und so bekommen wir also als geeignete Werthe von m unter 200:

m = 7, 9, 13, 19, 31, 37, 43, 61, **63**, 67, 73, 79, **91**, 97, 103, 109, **117**, 127, **133**, 139, 151, 157, 163, **171**, 181, 193, 199,

unter denen die Zahlen mit mehreren Primtheilern durch fetten Druck ausgezeichnet sind. Die kleinste Zahl m, in der mehr als zwei Primzahlen aufgehen, ist $7 . 9 . 13 = 819$.

Verstehen wir also unter $q_1, q_2, q_3 \ldots$ Zahlen, die aus der Reihe der Zahlen 9 und der Primzahlen 7, 13, 19, 31 ... genommen sind, so ist der allgemeine Ausdruck für m:

(1) $$m = q_1 q_2 q_3 \ldots q_\mu.$$

Die Indexmoduln sind, wenn $q_1 = 9$ ist, $c_1 = 6$, $c_2 = q_2 - 1$, $c_3 = q_3 - 1 \ldots$ Wenn 9 und 7 unter den Factoren von m nicht vorkommen, so fällt der Indexmodul 6 weg.

Die Grössen $\delta_{1,1}, \delta_{1,2}, \ldots \delta_{1,\mu}$ sind die grössten gemeinschaftlichen Theiler von $i_1 = 3$ mit den $c_1, c_2, \ldots c_\mu$; sie sind also alle $= 3$, und es folgt nach §. 21, (11):

$$i_{1,h} = 1, \quad c_{1,h} = {}^1/_3\, c_1.$$

Die Matrix §. 21, (24) besteht hier nur aus der einen Verticalreihe $e_{1,1}, e_{1,2}, \ldots e_{1,\mu}$, und diese Grössen kann man beliebig wählen, wenn nur wenigstens eine darunter ist, die durch 3 untheilbar ist. Diese Zahlen $e_{1,1}, e_{1,2}, \ldots e_{1,\mu}$ sind übrigens nur nach dem Modul 3 bestimmt, und können also gleich 0, 1 oder 2 angenommen werden. Die Bedingung 6. des §. 21 verlangt aber auch, dass, wenn $q_1 = 9$ ist, $c_{1,1}\, e_{1,1} = 2\, e_{1,1}$ nicht durch 3 theilbar sein soll, und wenn q_2 eine Primzahl ist, dass

$$c_{1,2}\, e_{1,2} = {}^1/_3\, (q_2 - 1)\, e_{1,2}$$

nicht durch $q_2 - 1$ theilbar sei, d. h. also, es darf keine der Zahlen $e_{1,1}, e_{1,2}, \ldots e_{1,\mu}$ durch 3 theilbar sein, und wir können für jede von ihnen ± 1 wählen.

Um also die Indices $\alpha_1, \alpha_2, \ldots \alpha_\mu$ aller Zahlen a zu finden, die in der Periode

(2) $$\eta = \Sigma\, r^a$$

vorkommen können, hat man nach §. 22, (3) alle Zahlen α (nach dem Modul 3) zu nehmen, die einer Congruenz

(3) $$\pm \alpha_1 \pm \alpha_2 \pm \alpha_3 \cdots \pm \alpha_\mu \equiv 0 \pmod 3$$

genügen, wobei für eine bestimmte Gruppe eine Vorzeichen-Combination festgehalten werden muss.

Die Anzahl der möglichen cubischen Körper hängt bei gegebenem m nur von der Zahl μ der Indexmoduln ab und beträgt, da eines der Vorzeichen in (3) willkürlich angenommen werden kann, $2^{\mu-1}$.

Ganz ähnlich würde sich das Resultat gestalten, wenn man statt 3 eine andere Primzahl p für i_1 setzen würde. Es würde dann nur in die Congruenz (3) an Stelle der doppelten Vor-

zeichen je ein volles Restsystem von p (mit Ausschluss der 0) treten.

Wir wollen aber bei der Annahme $i_1 = 3$ stehen bleiben, und unter $\varepsilon_1, \varepsilon_2, \dots \varepsilon_\mu$ irgend eine Combination der Zahlen ± 1 verstehen. Dann können wir die Congruenz (3) auch so schreiben

(4) $$\varepsilon_1 \alpha_1 + \varepsilon_2 \alpha_2 + \cdots + \varepsilon_\mu \alpha_\mu \equiv 0 \pmod 3.$$

Die Zeichencombination $\varepsilon_1, \varepsilon_2, \dots \varepsilon_\mu$, in der ein Zeichen willkürlich angenommen werden kann, da die gleichzeitige Aenderung aller Vorzeichen in (4) nichts ändert, bestimmt die einzelne Gruppe $\mathfrak{A}$, und offenbar sind diese Gruppen $\mathfrak{A}$ auch alle von einander verschieden. Denn ist z. B. in einer Gruppe $\varepsilon_1 = \varepsilon_2 = +1$, in einer anderen $\varepsilon_1 = +1$, $\varepsilon_2 = -1$, so enthält die erste die Zahlencombination:

$$\alpha_1 \equiv 1,\ \alpha_2 \equiv -1,\ \alpha_3 \equiv 0, \dots \alpha_\mu \equiv 0 \pmod 3,$$

die in der zweiten nicht vorkommt.

Um die Gruppen $\mathfrak{A}$ definitiv zu finden, legt man ein System primitiver Wurzeln $g_1, g_2, \dots g_\mu$ von $q_1, q_2, \dots q_\mu$ zu Grunde und bestimmt a nach dem Modul m aus den Congruenzen:

(5) $$\begin{aligned} a &\equiv g_1^{\alpha_1} \pmod{q_1} \\ &\equiv g_2^{\alpha_2} \pmod{q_2} \\ &\dots\dots\dots \\ &\equiv g_\mu^{\alpha_m} \pmod{q_\mu}. \end{aligned}$$

Setzen wir, indem wir unter σ einen der Reste $0, \pm 1$ verstehen,

(6) $$\sigma \equiv \varepsilon_1 \nu_1 + \varepsilon_2 \nu_2 + \cdots + \varepsilon_\mu \nu_\mu \pmod 3,$$

so besteht $\mathfrak{A}$ aus allen Zahlen a, deren Indices $\nu_1 = \alpha_1$, $\nu_2 = \alpha_2$, $\dots \nu_\mu = \alpha_\mu$ der Bedingung $\sigma = 0$ genügen. Die beiden anderen Werthe $\sigma = 1$, $\sigma = -1$ bestimmen die beiden Nebengruppen $\mathfrak{A}'$, $\mathfrak{A}''$ von $\mathfrak{A}$, so dass

$$\mathfrak{R} = \mathfrak{A} + \mathfrak{A}' + \mathfrak{A}''$$

ist. Ist a' und a'' je eine Zahl aus $\mathfrak{A}'$ und $\mathfrak{A}''$, so ist $\mathfrak{A}' = \mathfrak{A} a'$, $\mathfrak{A}'' = \mathfrak{A} a''$.

Wir bezeichnen nun mit η die Kreistheilungsperiode, die zu $\mathfrak{A}$ gehört, und mit η', η'' die conjugirten Perioden, also

(7) $$\eta = \sum r^a,\quad \eta' = \sum r^{a'},\quad \eta'' = \sum r^{a''}.$$

Wenn dann ϱ eine imaginäre dritte Einheitswurzel ist, so erhalten wir die Resolvente

$$(\varrho, \eta) = \eta + \varrho\, \eta' + \varrho^2 \eta'',$$

und dafür können wir mit Benutzung der Bezeichnung (6) setzen

$$(8) \qquad (\varrho, \eta) = \sum^{n} \varrho^{\sigma} r^{n},$$

worin n alle Zahlen der Gruppe $\mathfrak{N}$ durchläuft, und in σ für $\nu_1, \nu_2 \dots \nu_\mu$ jedesmal die Indices von n zu setzen sind.

Es mögen nun mit $r_1, r_2, \dots r_\mu$ primitive Einheitswurzeln der Grade $q_1, q_2, \dots q_\mu$ bezeichnet sein, und

$$r = r_1 r_2, \dots r_\mu$$

gesetzt werden. Dann lässt sich der Ausdruck (8) in ein Product zerlegen, nämlich, wenn wir

$$n \equiv n_h \pmod{q_h}$$

setzen, in:

$$(9) \qquad (\varrho, \eta) = \sum \varrho^{\varepsilon_1 \nu_1} r_1^{n_1} \sum \varrho^{\varepsilon_2 \nu_2} r_2^{n_2} \dots \sum r_\mu^{\varepsilon_\mu \nu_\mu} r_\mu^{n_\mu}.$$

Die Factoren dieses Productes sind nun genau die Resolventen, die wir in §. 172 des ersten Bandes untersucht haben, und wir erhalten, wenn wir

$$(10) \qquad \sum^{n_1} \varrho^{\nu_h} r^{n_h} = (\varrho, \eta_h), \quad h = 1, 2, \dots \mu$$

setzen:

$$(11) \qquad (\varrho, \eta) = (\varrho^{\varepsilon_1}, \eta_1)(\varrho^{\varepsilon_2}, \eta_2) \dots (\varrho^{\varepsilon_\mu}, \eta_\mu).$$

Wenn wir hierauf die Formeln (5), (6), (25), (26) des eben angeführten Paragraphen anwenden, so erhalten wir:

$$(12) \qquad (\varrho, \eta)(\varrho^{-1}, \eta) = m,$$

$$(13) \qquad (\varrho, \eta)^3 = m(a + b\varrho), \quad (\varrho^2, \eta)^3 = m(a + b\varrho^2),$$

worin a und b gewisse ganze Zahlen sind, die sich aus den genannten Formeln berechnen lassen, die aber nach der Wahl der ε verschieden ausfallen.

Aus (12) und (13) folgt dann noch:

$$(14) \qquad m = a^2 - ab + b^2.$$

Hiernach können wir die cubische Gleichung aufstellen, deren Wurzeln die Grössen η, η', η'' sind. Sie möge lauten:

$$(15) \qquad \eta^3 - \alpha\eta^2 + \beta\eta - \gamma = 0,$$

worin α, β, γ ganze Zahlen sind. Was zunächst α betrifft, so ist es gleich der Summe aller primitiven m^{ten} Einheitswurzeln, also

$$\alpha = \sum r_1 \sum r_2 \dots \sum r_\mu,$$

und dieser Werth ist $= 0$ oder $= (-1)^\mu$, je nachdem 9 unter den Factoren von m vorkommt oder nicht. Die beiden anderen Coëfficienten lassen sich ganz so berechnen, wie an der er-

wähnten Stelle gezeigt ist. Wir wollen hier die Rechnung in etwas veränderter Form anordnen. Wir setzen:

$$\zeta = \eta - \frac{\alpha}{3},$$

was zur Folge hat, dass $(\varrho, \eta) = (\varrho, \zeta)$ ist, wegen $1 + \varrho + \varrho^2 = 0$. Dann ergiebt sich für ζ die cubische Gleichung:

(16) $$\zeta^3 + P\zeta - Q = 0,$$

worin

(17) $$P = \beta - \frac{\alpha^2}{3}, \quad Q = \frac{2\alpha^3}{27} - \frac{\alpha\beta}{3} + \gamma.$$

Nun ergiebt sich aus (12):

$$(\varrho, \zeta)(\varrho^{-1}, \zeta) = m = \zeta^2 + \zeta'^2 + \zeta''^2 - \zeta\zeta' - \zeta\zeta'' - \zeta'\zeta''$$
$$= -3P$$

oder

(18) $$P = -\frac{m}{3},$$

und aus (13), nach einigen einfachen Rechnungen, wenn

$$S = \zeta^2\zeta' + \zeta'^2\zeta'' + \zeta''^2\zeta, \quad S' = \zeta\zeta'^2 + \zeta'\zeta''^2 + \zeta''\zeta^2$$

gesetzt wird:

$$m(a + b\varrho) = 9Q + 3\varrho S + 3\varrho^2 S'$$
$$m(a + b\varrho^2) = 9Q + 3\varrho^2 S + 3\varrho S'$$
$$0 = 9Q + 3S + 3S',$$

woraus durch Addition:

(19) $$27Q = m(2a - b),$$

und durch Subtraction der beiden ersten:

(20) $$mb = 3(S - S') = 3(\zeta - \zeta')(\zeta'' - \zeta)(\zeta'' - \zeta').$$

Wenn m durch 9 theilbar ist, so ist $\alpha = 0$, und P und Q sind g a n z e Zahlen und P durch 3 theilbar. Ist aber m nicht durch 9 theilbar, so sind erst $3P$ und $27Q$ ganze, nicht durch 3 theilbare Zahlen.

Ist D die Discriminante der Gleichung (15), also eine ganze Zahl, so ist auch

(21) $$\sqrt{D} = (\eta - \eta')(\eta'' - \eta)(\eta'' - \eta') = (\zeta - \zeta')(\zeta'' - \zeta)(\zeta'' - \zeta')$$
$$= \frac{mb}{3}$$

eine ganze Zahl, und also ist, wenn m nicht durch 9 theilbar ist, b durch 3 theilbar. Nun ist nach (14)

$$(22) \qquad 4m = (2a - b)^2 + 3b^2,$$

und wenn m durch 9 theilbar ist, so ist $2a - b$ nach (19) durch 3 theilbar, und aus (22) folgt dann, dass auch in diesem Falle b durch 3 theilbar ist. Wir können also in allen Fällen setzen

$$2a - b = A, \quad b = 3B,$$

so dass A, B ganze Zahlen sind, die der Bedingung

$$(23) \qquad 4m = A^2 + 27B^2$$

genügen, und die Gleichung für ζ wird dann

$$(24) \qquad \zeta^3 - \frac{m}{3}\zeta - \frac{mA}{27} = 0,$$

und für die Discriminante dieser Gleichung folgt

$$(25) \qquad \sqrt{D} = mB.$$

Um für die einfachsten Beispiele die Rechnung durchzuführen, nehmen wir für $q_1 = 9$, $q_2 = 7$, $q_3 = 13$ aus §. 172 des ersten Bandes die Werthe:

$$\begin{aligned} q_1 &= 9, & a + b\varrho &= 3\varrho, \\ q_2 &= 7, & a + b\varrho &= -(1 + 3\varrho), \\ q_3 &= 13, & a + b\varrho &= -(4 + 3\varrho). \end{aligned}$$

Daraus ergeben sich für $m = 63$ die beiden Werthe:

$$\begin{aligned} m = 63:\ a + b\varrho &= -3\varrho(1 + 3\varrho) = 9 + 6\varrho, \\ a + b\varrho &= -3\varrho(1 + 3\varrho^2) = -9 - 3\varrho, \end{aligned}$$

für

$$\begin{aligned} m = 91:\ a + b\varrho &= (1 + 3\varrho)(4 + 3\varrho) = -5 + 6\varrho, \\ a + b\varrho &= (1 + 3\varrho)(4 + 3\varrho^2) = 10 + 9\varrho, \end{aligned}$$

und für $m = 819$ die Werthe:

$$\begin{aligned} a + b\varrho &= 3\varrho(1 + 3\varrho)(4 + 3\varrho) = -3(6 + 11\varrho), \\ &= 3\varrho(1 + 3\varrho)(4 + 3\varrho^2) = -3(9 - \varrho), \\ &= 3\varrho(1 + 3\varrho^2)(4 + 3\varrho) = 3(9 + 10\varrho), \\ &= 3\varrho(1 + 3\varrho^2)(4 + 3\varrho^2) = 3(6 - 5\varrho). \end{aligned}$$

Daraus finden sich die cubischen Gleichungen für η in diesen drei Fällen:

$$\begin{aligned} m = 63:\ & \eta^3 - 21\eta - 28 = 0, \qquad (\eta = \zeta) \\ & \eta^3 - 21\eta + 35 = 0, \\ m = 91:\ & \eta^3 - \eta^2 - 30\eta + 64 = 0, \quad (\eta = \zeta + 1/3) \\ & \eta^3 - \eta^2 - 30\eta - 27 = 0, \end{aligned}$$

$$m = 819:\quad \eta^3 - 273\eta + 91 \quad = 0, \qquad (\eta = \zeta)$$
$$\eta^3 - 273\eta + 91.19 = 0,$$
$$\eta^3 - 273\eta + 91.\ 8 = 0,$$
$$\eta^3 - 273\eta + 91.17 = 0.$$

Die Wurzeln dieser einzelnen Gleichungen findet man am besten aus der Gleichung (9) oder (11), indem man darin nach Potenzen von ϱ ordnet, dabei aber nur $\varrho^3 = 1$, nicht $\varrho^2 + \varrho + 1 = 0$ benutzt.

So bekommt man z. B. für den Fall $m = 63$:

$$(\varrho, \eta) = (\eta_1 + \varrho\,\eta_1' + \varrho^2\eta_1'')\,(\eta_2 + \varrho\,\eta_2' + \varrho^2\eta_2'')$$

oder

$$= (\eta_1 + \varrho\,\eta_1' + \varrho^2\eta_1'')\,(\eta_2 + \varrho\,\eta_2'' + \varrho^2\eta_2'),$$

worin

$$\eta_1 = r_1 + r_1^{-1},\quad \eta_1' = r_1^2 + r_1^{-2},\quad \eta_1'' = r_1^4 + r_1^{-4}$$
$$\eta_2 = r_2 + r_2^{-1},\quad \eta_2' = r_2^3 + r_2^{-3},\quad \eta_2'' = r_2^9 + r_2^{-9}$$

zu setzen ist (Bd. I, §. 172), und man findet so:

$$\eta = \eta_1\eta_2 + \eta_1'\eta_2'' + \eta_1''\eta_2'$$

oder

$$\eta = \eta_1\eta_2 + \eta_1'\eta_2' + \eta_1''\eta_2''.$$

Um die Gruppen $\mathfrak{A}$ daraus zu finden, hat man zwei Zahlen x, y so zu bestimmen, dass $7x + 9y = 1$ wird, und dann

$$r = r_1 r_2,\quad \text{also}\quad r_1 = r^{7x},\ r_2 = r^{9y}$$

zu setzen. Nimmt man $x = 4$, $y = -3$ an, so erhält man für x die beiden Werthe von η:

$$\eta = (r^{28} + r^{-28})\,(r^{27} + r^{-27}) + (r^7 + r^{-7})\,(r^9 + r^{-9})$$
$$+ (r^{14} + r^{-14})\,(r^{18} + r^{-18})$$
$$\eta = (r^{28} + r^{-28})\,(r^{27} + r^{-27}) + (r^7 + r^{-7})\,(r^{18} + r^{-18})$$
$$+ (r^{14} + r^{-14})\,(r^9 + r^{-9}),$$

also

$$\mathfrak{A} = \pm 1,\ \pm 8,\ \pm 2,\ \pm 16,\ \pm 4,\ \pm 32,$$

oder

$$\mathfrak{A} = \pm 1,\ \pm 8,\ \pm 11,\ \pm 25,\ \pm 5,\ \pm 23.$$

Die beiden Gruppen können durch die Potenzen von 2 und von 11 dargestellt werden.

Die cubischen Gleichungen, deren Bildungsgesetze wir jetzt kennen gelernt haben, enthalten mit ihren Tschirnhausen-Transformationen alle cubischen Kreistheilungsgleichungen. Aber diese Gleichungen sind auch alle von einander

verschieden und können nicht durch Tschirnhausen-Transformation in einander übergeführt werden, weil sie zu primären Theilern von verschiedenen vollen Kreistheilungskörpern gehören, oder, wenn sie in demselben vollen Kreistheilungskörper enthalten sind, verschiedene Gruppen haben.

Man kann freilich noch aus anderen Einheitswurzeln Kreistheilungsperioden bilden, die zu cubischen Gleichungen führen. Diese Perioden können aber durch niedrigere Einheitswurzeln ausgedrückt werden, und sind nicht primär. So erhält man z. B., wenn r eine 35[ste] Einheitswurzel ist, eine Periode von 8 Gliedern, deren Exponenten aus den Potenzen von -8 gebildet sind:

$$\eta = r + r^{-1} + r^6 + r^{-6} + r^8 + r^{-8} + r^{13} + r^{-13},$$

die also auch einer cubischen Gleichung genügt.

Es ist aber

$$1 + r^7 + r^{-7} + r^{14} + r^{-14} = 0,$$

und wenn man diese Gleichung mit $(r^{15} + r^{-15})$ multiplicirt:

$$r^{15} + r^{-15} + r + r^{-1} + r^6 + r^{-6} + r^8 + r^{-8} + r^{13} + r^{-13} = 0,$$

also

$$\eta = -(r^{15} + r^{-15}),$$

was unter den Perioden der 7[ten] Einheitswurzeln schon vorkommt. Diese Erscheinung erklärt sich daraus, dass $m = 35$ nicht die in §. 21 verlangte Eigenschaft hat, dass $q - 1$ für alle in m aufgehenden Primzahlen q durch 3 theilbar ist.

§. 24.

Biquadratische Kreistheilungskörper.

Bei den biquadratischen Kreistheilungsgleichungen hat man zwei Arten zu unterscheiden. Wir können zwei Invarianten $i_1 = i_2 = 2$ oder nur eine Invariante $i_1 = 4$ annehmen. Wir wollen den ersten Fall voranschicken.

Für m haben wir in diesem Falle nach der Zusammenstellung §. 21 folgende Bedingungen:

m kann ungerade sein, durch 4 oder durch 8, aber durch keine höhere Potenz von 2 theilbar sein. Keine ungerade Primzahl kann mehr als einmal in m aufgehen, und es müssen mindestens zwei Indexmoduln vorhanden sein; also müssen ausser in

dem Falle $m = 8$ mindestens zwei verschiedene Primzahlen in m enthalten sein.

Setzen wir:

$$m = q_1\, q_2 \,.\,.\,.\, q_\mu,$$

wenn m ungerade oder nur durch 4 theilbar ist,

$$m = q_2\, q_3 \,.\,.\,.\, q_\mu,$$

wenn m durch 8 theilbar ist, so dass $q_1 = 4$ sein kann und in der zweiten Formel $q_2 = 8$ ist, während die übrigen q ungerade Primzahlen sind, so sind die Indexmoduln in den drei Fällen:

$$\begin{array}{llll} & q_1 - 1, & q_2 - 1, \ldots, & q_\mu - 1 \\ & 2\quad, & q_2 - 1, \ldots, & q_\mu - 1 \\ 2, & 2\quad, & q_3 - 1, \ldots, & q_\mu - 1. \end{array}$$

Weil hiernach alle Indexmoduln durch 2 theilbar sind, so sind die Bedingungen für m erschöpft.

Es ist [§. 21, (11)]:

(1) $\delta_{k,h} = 2,\ i_{k,h} = 1,\ c_{k,h} = {}^1/_2\, c_h,\ k = 1, 2,\ h = 1, 2, \ldots \mu.$

Nun hat man die Grössen $e_{k,h}$ so zu bestimmen, dass aus der Matrix

(2) $$\begin{array}{l} e_{1,1},\ e_{1,2},\ .\,.\,.\ e_{1,\mu} \\ e_{2,1},\ e_{2,2},\ .\,.\,.\ e_{2,\mu} \end{array}$$

wenigstens eine ungerade zweireihige Determinante gebildet werden kann.

Damit $\mathfrak{A}$ primärer Theiler von $\mathfrak{N}$ sei, kommt noch die Bedingung §. 21, 6. hinzu, wo nun zu unterscheiden ist, ob m durch 8 theilbar ist oder nicht. Ist m durch 8 theilbar, so ist die Anzahl der Indexmoduln um eins grösser, als die Anzahl der Primfactoren von m, und es giebt einen Indexmodul, dem kein Primfactor von m entspricht; im anderen Falle stimmen beide Zahlen überein. Nach §. 21, 6. hat man die $e_{k,h}$ so zu wählen, dass in keinem der Paare

$$e_{1,1},\ e_{2,1};\ e_{1,2},\ e_{2,2};\ .\,.\,.\ e_{1,\mu},\ e_{2,\mu},$$

denen ein Primfactor von m entspricht, beide Zahlen gerade sind. Wenn m durch 8 theilbar ist, so ist ein dem Indexmodul $c_k = 2$ entsprechendes Paar darunter, dem keine solche Beschränkung auferlegt ist.

Sind die Zahlen $e_{k,h}$ (nach dem Modul 2) so bestimmt, so

erhält man nach §. 22 für die Indices der Zahlen in $\mathfrak{A}$ die beiden Congruenzen:

$$(3)\qquad \begin{matrix} e_{1,1}\alpha_1 + e_{1,2}\alpha_2 + \cdots + e_{1,\mu}\alpha_\mu \equiv 0 \\ e_{2,1}\alpha_1 + e_{2,2}\alpha_2 + \cdots + e_{2,\mu}\alpha_\mu \equiv 0 \end{matrix} \pmod 2.$$

Um die Zahl der möglichen Gruppen $\mathfrak{A}$ zu ermitteln, bedenke man, dass man die Relationen (3), ohne ihren Inhalt zu ändern, durch zwei von einander unabhängige lineare Combinationen ersetzen kann. Danach kann man eines der Zahlenpaare in der Matrix (2), z. B. $e_{1,1}, e_{2,1} = 1, 0$ annehmen und so für (2) setzen:

$$\begin{matrix} 1, & e_{1,2}, & \ldots & e_{1,\mu} \\ 0, & e_{2,2}, & \ldots & e_{2,\mu}. \end{matrix}$$

Jetzt kann man für die $e_{2,2} \ldots e_{2,\mu}$ irgend eine Combination der Zahlen 0, 1 setzen, mit Ausnahme der einen, bei der alle $e_{2,h} = 0$ werden. Zu jedem $e_{2,h} = 0$ muss das zugehörige $e_{1,h} = 1$ sein, während einem $e_{2,h} = 1$ ein $e_{1,h} = 0$ oder $= 1$ entsprechen kann. Die Anzahl der auf diese Weise entstandenen Combinationen ist:

$$1 + (\mu - 1)2 + \frac{(\mu - 1)(\mu - 2)}{1.2} 2^2 + \cdots + 2^{\mu-1} - 1 = 3^{\mu-1} - 1.$$

Nun kann man aber die zweite der Gleichungen (3), ohne ihre Bedeutung zu ändern, zu der ersten noch addiren, so dass also je zwei der gewonnenen Combinationen dieselbe Gruppe ergeben. Es bleiben also

$$(4)\qquad \frac{3^{\mu-1} - 1}{2}$$

verschiedene Combinationen der $e_{h,k}$, die auch, wie leicht einzusehen ist, zu verschiedenen Gruppen $\mathfrak{A}$ führen. Denn angenommen, man habe das eine Mal $e_{1,2}, e_{2,2} = 1, 0$, das andere Mal $= 0, 1$ genommen, so genügt der ersten Annahme $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = 0, \ldots \alpha_\mu = 0$, was der zweiten nicht genügt.

Die Zahl, die wir eben bestimmt haben, ist nur dann erschöpfend, wenn m nicht durch 8 theilbar ist, weil dabei angenommen ist, dass dabei niemals $e_{1,h}, e_{2,h} = 0, 0$ sei. Wenn aber m durch 8 theilbar ist, dann kann bei einem Paare diese Werthcombination vorkommen, und wir müssen also noch die Fälle hinzufügen, die durch

$$\begin{matrix} 1 & 0 & e_{1,3} & \ldots & e_{1,\mu} \\ 0 & 0 & e_{2,3} & \ldots & e_{2,\mu} \end{matrix}$$

angedeutet sind, und deren Zahl man ebenso wie oben

$$= \frac{3^{\mu-2}-1}{2}$$

findet. Wenn also m durch 8 theilbar ist, so ist die Gesammtzahl der Gruppen $\mathfrak{A}$

$$(5) \qquad \frac{3^{\mu-1}-1}{2} + \frac{3^{\mu-2}-1}{2} = 2.3^{\mu-2} - 1.$$

Die kleinsten Werthe, die m in diesem Falle annehmen kann, sind

$$m = 8, 12, 15, 20, 21, 24, 28, 33, 35, 39, 40, 44 \ldots$$

Die kleinste Zahl, die zu mehr als einer solchen Gruppe Anlass giebt, ist $m = 24$, für die man $\mu = 3$ hat, und die also nach (5) fünf verschiedene Gruppen giebt. Man erhält nämlich folgende zulässige und von einander verschiedene Combinationen der $e_{h,k}$:

$$\begin{matrix} 1\,0\,1 & 1\,1\,0 & 1\,1\,0 & 1\,0\,0 & 1\,0\,0 \\ 0\,1\,0, & 0\,0\,1, & 0\,1\,1, & 0\,1\,1, & 0\,0\,1, \end{matrix}$$

was zu folgenden Bestimmungen über die Indices führt:

$$\begin{matrix} \alpha_1 \equiv \alpha_3, & \alpha_2 \equiv 0, & \\ \alpha_1 \equiv \alpha_2, & \alpha_3 \equiv 0, & \\ \alpha_1 \equiv \alpha_2 \equiv \alpha_3, & & \pmod 2 \\ \alpha_1 \equiv 0, & \alpha_2 \equiv \alpha_3 & \\ \alpha_1 \equiv 0, & \alpha_3 \equiv 0, & \end{matrix}$$

und wenn man also die Zahlen a durch die Congruenzen

$$a \equiv (-1)^{\alpha_2} 5^{\alpha_1} \pmod 8, \quad a \equiv 2^{\alpha_3} \pmod 3)$$

bestimmt, so ergeben sich folgende fünf zweigliedrige Gruppen:

$$\begin{aligned} \mathfrak{A}_1 &= 1,\ 5 \\ \mathfrak{A}_2 &= 1,\ 19 \\ \mathfrak{A}_3 &= 1,\ 11 \\ \mathfrak{A}_4 &= 1,\ 23 \\ \mathfrak{A}_5 &= 1,\ 7. \end{aligned}$$

Um die Perioden η zu berechnen, können wir ähnlich verfahren, wie im vorigen Paragraphen. Wir bezeichnen mit $\nu_1, \nu_2, \ldots \nu_\mu$ die Indices einer Zahl n und setzen

$$\begin{aligned} e_{1,1}\nu_1 + e_{1,2}\nu_2 + \cdots + e_{1,\mu}\nu_\mu &= \sigma_1, \\ e_{2,1}\nu_1 + e_{2,2}\nu_2 + \cdots + e_{2,\mu}\nu_\mu &= \sigma_2, \end{aligned}$$

und erhalten, wenn $\varepsilon_1, \varepsilon_2$ den Werth 0 oder 1 haben, die Resolventen

$$
\begin{aligned}
(6) \qquad \Omega_{\varepsilon_1, \varepsilon_2} &= \sum^{n} (-1)^{\varepsilon_1 \sigma_1 + \varepsilon_2 \sigma_2} r^n \\
&= \eta + (-1)^{\varepsilon_1} \eta' + (-1)^{\varepsilon_2} \eta'' + (-1)^{\varepsilon_1 + \varepsilon_2} \eta'''.
\end{aligned}
$$

Ist nun $m = q_1 q_2 \dots q_\mu$ nicht durch 8 theilbar, so können wir, wenn $r_1, r_2, \dots r_\mu$ primitive Wurzeln der Grade $q_1, q_2, \dots q_\mu$ bedeuten,

$$r = r_1 r_2 \dots r_\mu$$

setzen, ferner

$$
\begin{aligned}
n &\equiv n_1 \pmod{q_1} \\
&\equiv n_2 \pmod{q_2} \\
&\dots\dots\dots \\
&\equiv n_\mu \pmod{q_\mu},
\end{aligned}
$$

wodurch sich ergiebt:

$$(7) \qquad \Omega_{\varepsilon_1, \varepsilon_2} = \prod_{1, \mu}^{h} \sum^{n_h} (-1)^{\nu_h (\varepsilon_1 e_{1h} + \varepsilon_2 e_{2h})} r_h^{n_h}.$$

Die einzelnen Factoren dieses Productes sind die in §. 171 (Bd. I) bestimmten Gauss'schen Summen, die dort durch Quadratwurzeln ausgedrückt sind. Nur wenn $q_1 = 4$ ist und $\varepsilon_1 e_{1,1} + \varepsilon_2 e_{1,2} = 0$, ist $\Omega_{\varepsilon_1, \varepsilon_2} = 0$.

Ist aber m durch 8 theilbar und

$$m = q_2 q_3 \dots q_\mu, \quad q_2 = 8,$$

so erhält man, wenn man $r = r_2 r_3 \dots r_\mu$ setzt:

$$
\begin{aligned}
\Omega_{\varepsilon_1, \varepsilon_2} = &\sum^{n_2} (-1)^{\varepsilon_1 (e_{1,1} \nu_1 + e_{1,2} \nu_2)} (-1)^{\varepsilon_2 (e_{2,1} \nu_1 + e_{2,2} \nu_2)} r_2^{n_2} \\
&\times \prod_{3, \mu}^{h} \sum^{n_h} (-1)^{\nu_h (\varepsilon_1 e_{1,h} + \varepsilon_2 e_{2,h})} r_h^{n_h}.
\end{aligned}
$$

In den fünf oben aufgestellten Gruppen, die zu $m = 24$ gehören, kann man die Perioden aus dieser Formel oder auch leicht direct berechnen, wenn man

$$r = e^{\frac{\pi i}{12}} = e^{\frac{\pi i}{3}} e^{-\frac{\pi i}{4}}$$

setzt. Man erhält dann für die fünf Grössen:

$$\mathfrak{A}_1) \qquad \eta = \frac{(1 + i) \sqrt{3}}{\sqrt{2}}$$

$$\mathfrak{A}_3) \qquad \eta = i\,\frac{\sqrt{3}-1}{\sqrt{2}}$$

$$\mathfrak{A}_4) \qquad \eta = \frac{1+\sqrt{3}}{\sqrt{2}}$$

$$\mathfrak{A}_5) \qquad \eta = \frac{1+i\sqrt{3}}{\sqrt{2}}.$$

Es soll nun zuletzt noch der Fall einer einzigen Invariante $i_1 = 4$ betrachtet werden. Die Bedingungen für m bestehen dann einfach darin, dass m durch 4, 8, 16, aber keine höhere Potenz von 2 theilbar sein kann, dass ungerade Primzahlen nur einfach in m aufgehen können, und dass mindestens einer der Indexmoduln durch 4 theilbar sein muss. Die ersten Werthe sind also

$$m = 5, 13, 15, 16, 17, 20, 29, 33, 37, 39, 40 \ldots$$

Wir wollen annehmen, es seien von den Indexmoduln $c_1, c_2, \ldots c_\varrho$ durch 4 theilbar, $c_{\varrho+1}, c_{\varrho+2}, \ldots c_\mu$ durch 2, aber nicht durch 4 theilbar. Es muss dann ϱ mindestens gleich 1 sein, und folglich ist

$$\delta_{1,1} = \delta_{1,2} = \cdots = \delta_{1,\varrho} = 4, \quad \delta_{1,\varrho+1} = \quad \cdots = \delta_{1,\mu} = 2$$

$$i_{1,1} = i_{1,2} = \cdots = i_{1,\varrho} = 1, \quad i_{1,\varrho+1} = \quad \cdots = i_{1,\mu} = 2$$

$$c_{1,1} = \frac{c_1}{4}, \;\cdots\cdots,\; c_{1,\varrho} = \frac{c_\varrho}{4},\; c_{1,\varrho+1} = \frac{c_{\varrho+1}}{2}, \;\cdots,\; c_{1,\mu} = \frac{c_\mu}{2}.$$

Nun sind die $e_{1,h}$ so zu bestimmen, dass von den Zahlen

$$e_{1,1}, e_{1,2}, \ldots e_{1,\varrho}$$

wenigstens eine ungerade ist, und dass (wegen §. 21, 6.) von den Zahlen

$$e_{1,1}, e_{1,2}, \ldots e_{1,\varrho}$$

keine durch 4, und von den

$$e_{1,\varrho+1}, e_{1,\varrho+2}, \ldots e_{1,\mu}$$

keine durch 2 theilbar sei. Eine Ausnahme bildet hierbei wieder im Falle, wo m durch 8 oder durch 16 theilbar ist, die Zahl $e_{1,h}$, der keiner der Primfactoren von m entspricht, die auch gerade sein kann.

Dann erhalten wir für die Indices α der Zahlen a die Congruenz:

$$e_{1,1}\alpha_1 + \cdots + e_{1,\varrho}\alpha_\varrho + 2(e_{1,\varrho+1}\alpha_{\varrho+1} + \cdots + e_{1,\mu}\alpha_\mu) \equiv 0 \pmod 4.$$

Nehmen wir als Beispiel $m = 48$, so haben wir zwei Möglichkeiten, nämlich:

$$e_{1,1} = 1, \quad e_{1,2} = 0, \quad e_{1,3} = 1$$
$$e_{1,1} = 1, \quad e_{1,2} = 1, \quad e_{1,3} = 1,$$

und man findet aus ihnen die beiden Gruppen:

$$\mathfrak{A}_1 = 1,\ 17,\ 31,\ 47$$
$$\mathfrak{A}_2 = 1,\ \ 7,\ 41,\ 47.$$

§. 25.

Cubische Abel'sche Gleichungen.

Wir wollen diese Betrachtungen über die cubischen und biquadratischen Kreistheilungsgleichungen mit dem Beweise eines merkwürdigen Satzes abschliessen, der geeignet ist, diesen Gleichungen ein weit höheres und allgemeineres Interesse zu verleihen und der ein specieller Fall eines ganz allgemeinen Satzes ist, den wir erst später kennen lernen werden.

Der Satz lautet so:

Alle cubischen und biquadratischen Abel'schen Gleichungen im Körper der rationalen Zahlen sind Kreistheilungsgleichungen.

Dadurch gewinnen die Resultate der beiden letzten Paragraphen einen höheren Werth. Es folgt dann nämlich, dass durch die dort gebildeten Kreistheilungsperioden η alle Abel'schen Zahlkörper dritten und vierten Grades dargestellt sind, dass andere als die dort besprochenen Körper dieser Art nicht existiren.

Die Möglichkeit, diesen Satz für die speciellen Fälle der cubischen und biquadratischen Gleichungen einfach und ohne weitere Vorbereitung zu beweisen, beruht darauf, dass in den Körpern der dritten und vierten Einheitswurzeln $R(\varrho)$, $R(i)$ dieselben Gesetze der Zerlegung der Zahlen in ihre Primfactoren gelten, wie in den Körpern der rationalen Zahlen, wie in den §§. 173, 174 des ersten Bandes nachgewiesen ist. Es ist darum auch von Interesse, diese besonderen Fälle genauer zu betrachten, weil dadurch der Gang und das Ziel des später beizubringenden allgemeinen Beweises deutlicher erkannt wird.

Beginnen wir also mit den cubischen Gleichungen, und verstehen unter x_0, x_1, x_2 die Wurzeln irgend einer Abel'schen Gleichung dritten Grades. Da 3 eine Primzahl ist, so muss die Gleichung cyklisch sein, d. h. die cyklischen Functionen der Grössen x_0, x_1, x_2 sind rationale Zahlen.

Bezeichnen wir mit ϱ eine imaginäre dritte Einheitswurzel, so haben wir die beiden Resolventen

$$(1) \qquad \begin{aligned} (\varrho\,, x_0) &= x_0 + \varrho\, x_1 + \varrho^2 x_2 \\ (\varrho^2, x_0) &= x_0 + \varrho^2 x_1 + \varrho\, x_2, \end{aligned}$$

deren Cuben also Zahlen des Körpers $R(\varrho)$ und deren Product eine rationale Zahl sein muss.

Wir setzen demnach, indem wir mit a, b, c rationale (ganze oder gebrochene) Zahlen bezeichnen,

$$(2) \qquad \begin{aligned} (\varrho\,, x_0)^3 &= a + b\,\varrho \\ (\varrho^2, x_0)^3 &= a + b\,\varrho^2 \\ (\varrho\,, x_0)\,(\varrho^2, x_0) &= c, \end{aligned}$$

also auch

$$(3) \qquad (a + b\,\varrho)\,(a + b\,\varrho^2) = c^3.$$

Nun haben wir im Körper $R(\varrho)$ ausser den sechs Einheiten

$$\pm 1, \quad \pm \varrho, \quad \pm \varrho^2,$$

die alle als Potenzen von $-\varrho$ dargestellt werden können, die Primzahlen $\sqrt{-3} = \varrho - \varrho^2$, die reellen Primzahlen q von der Form $3N + 2$ und die beiden complexen Factoren der reellen Primzahlen p von der Form $3N + 1$. Die Zerlegung dieser Primzahlen in die beiden complexen Factoren π, π':

$$(4) \qquad p = \pi\,\pi'$$

haben wir im §. 172 des ersten Bandes dargestellt in der Form

$$(5) \qquad p = \psi_1(\varrho)\,\psi_1(\varrho^2).$$

Wir können also

$$(6) \qquad \pi = \psi_1(\varrho), \quad \pi' = \psi_1(\varrho^2),$$

setzen und haben dadurch unter den verschiedenen zu π associirten Zahlen eine bestimmte ausgewählt, und diese Zahlen π, π' stehen in einer bestimmten Beziehung zu den Kreistheilungsperioden der p^{ten} Einheitswurzeln η:

$$(7) \qquad (\varrho, \eta)^3 = p\,\pi, \quad (\varrho^2, \eta)^3 = p\,\pi'$$

[Bd. I, §. 172, (5)].

Nun ist $a + b\varrho$ eine ganze oder gebrochene Zahl des Körpers $R(\varrho)$. Wenn wir Zähler und Nenner dieser Zahl in ihre Primfactoren zerlegen, gemeinsame Factoren wegheben, und wenn wir unter $q_1, q_2, \ldots$ reelle Primzahlen der Form $3N + 2$, unter $\pi_1, \pi_1', \pi_2, \pi_2', \ldots$ conjugirte Paare imaginärer Primzahlen der Form (6) verstehen, so erhalten wir

$$(8) \quad \begin{aligned} a + b\varrho &= (-\varrho)^\lambda \quad (\sqrt{-3})^n \, q_1^{s_1} q_2^{s_2} \ldots \pi_1^{t_1} \pi_1'^{t_1'} \pi_2^{t_2} \pi_2'^{t_2'} \ldots \\ a + b\varrho^2 &= (-\varrho^2)^\lambda (-\sqrt{-3})^n \, q_1^{s_1} q_2^{s_2} \ldots \pi_1^{t_1'} \pi_1'^{t_1} \pi_2^{t_2'} \pi_2'^{t_2} \ldots \end{aligned}$$

worin

$$\lambda, n, s_1, s_2 \ldots t_1, t_1', t_2, t_2' \ldots$$

ganze positive oder negative Zahlen sind.

Nun ist aber nach (3) das Product der beiden Zahlen (8) der Cubus einer rationalen Zahl, und dies giebt, da eine rationale Zahl nur auf eine Art in Primfactoren zerlegbar ist, die folgenden Bedingungen:

$$(8) \quad \begin{aligned} n \equiv 0, \quad s_1 \equiv 0, \quad s_2 \equiv 0 \ldots \\ t_1 + t_1' \equiv 0, \quad t_2 + t_2' \equiv 0 \ldots \end{aligned} \quad \pmod 3,$$

und wir setzen also

$$(9) \quad \begin{aligned} n = 3\mu, \quad s_1 = 3\sigma_1, \quad s_2 = 3\sigma_2 \ldots \\ t_1 + t_1' = 3\tau_1, \quad t_2 + t_2' = 3\tau_2 \ldots, \end{aligned}$$

so dass $n, \sigma_1, \sigma_2 \ldots \tau_1, \tau_2 \ldots$ ganze Zahlen sind. Nun ist nach den Formeln (7):

$$(10) \quad \begin{aligned} \pi^t \pi'^{t'} &= p^{-(t+t')} (\varrho, \eta)^{3t} (\varrho^2, \eta)^{3t'} \\ \pi^{t'} \pi'^{t} &= p^{-(t+t')} (\varrho, \eta)^{3t'} (\varrho^2, \eta)^{3t}. \end{aligned}$$

Bezeichnen wir endlich noch mit ε eine 9te Einheitswurzel, so können wir

$$-\varrho = (-\varepsilon)^3$$

setzen, und stellen dadurch $a + b\varrho$ und $a + b\varrho^2$ als Cuben dar. Wir erhalten also nach (2):

$$(11) \quad (\varrho, x_0)^3 = (-\varepsilon)^{3\lambda} (\sqrt{-3})^{3\mu} q_1^{3\sigma_1} q_2^{3\sigma_2} \ldots p_1^{-3\tau_1} p_2^{-3\tau_2} H_1^3,$$

worin

$$(12) \quad H_1 = (\varrho, \eta_1)^{t_1} (\varrho^2, \eta_1)^{t_1'} (\varrho, \eta_2)^{t_2} (\varrho^2, \eta_2)^{t_2'} \ldots$$

eine Kreistheilungszahl ist. Bezeichnen wir mit H_2 die aus H_1 durch Vertauschung von ϱ mit ϱ^2 hervorgehende Zahl, so ist $H_1 H_2$ eine rationale Zahl.

Wenn wir aus (11) die dritte Wurzel ziehen, so folgt, da hierbei noch eine dritte Einheitswurzel ϱ_1 als Factor auftreten kann,

$$(13) \quad (\varrho, x_0) = (-\varepsilon)^\lambda \varrho_1 (\sqrt{-3})^\mu q_1^{\sigma_1} q_2^{\sigma_2} \ldots {}_1^{-\tau_1} p_2^{-\tau_2} \ldots H_1,$$

und ebenso erhalten wir

$$(14) \quad (\varrho^2, x_0) = (-\varepsilon^2)^\lambda \varrho_2 (-\sqrt{-3})^\mu q_1^{\sigma_1''} q_2^{\sigma_2''} \dots p_1^{-\tau_1} p_2^{-\tau_2} \dots H_2.$$

Weil das Product dieser beiden Ausdrücke rational sein muss, so ergiebt sich noch zwischen den Einheitswurzeln $\varrho, \varrho_1, \varrho_2$ die Relation

$$\varrho^\lambda \varrho_1 \varrho_2 = 1.$$

Setzen wir

$$(15) \quad x_0 + x_1 + x_2 = A,$$

so ist auch A eine rationale Zahl, und aus (13), (14), (15) folgt, dass

$$(16) \quad \begin{aligned} x_0 &= 1/3\,[A + (\varrho, x_0) + (\varrho^2, x_0)] \\ x_1 &= 1/3\,[A + \varrho^2 (\varrho, x_0) + \varrho\, (\varrho^2, x_0)] \\ x_2 &= 1/3\,[A + \varrho\, (\varrho, x_0) + \varrho^2 (\varrho^2, x_0)] \end{aligned}$$

Kreistheilungzahlen sind. Aus den Formeln (13), (14) können wir die Zusammensetzung dieser Zahlen aus den Perioden $\eta_1, \eta_2, \dots$ ersehen. Ein näheres Eingehen auf diesen Gegenstand ist aber nicht mehr erforderlich, weil wir schon im §. 23 alle Kreistheilungszahlen, die cubischen Gleichungen genügen, vollständig gebildet haben.

§. 26.

Biquadratische Abel'sche Gleichungen.

Ganz ähnlich kann der Beweis des entsprechenden Satzes für die biquadratischen Abel'schen Gleichungen geführt werden. Nur sind hier zwei Fälle zu unterscheiden, nämlich Gleichungen mit nicht cyklischer Gruppe, und Gleichungen mit cyklischer Gruppe.

Für die nicht cyklischen Abel'schen Gleichungen mit den Wurzeln x_0, x_1, x_2, x_3 ist die Gruppe:

$$(1) \quad 1, \ (0, 1)\,(2, 3), \ (0, 2)\,(1, 3), \ (0, 3)\,(1, 2),$$

und es sind also die drei Quadrate

$$(2) \quad \begin{aligned} (x_0 + x_1 - x_2 - x_3)^2 &= a \\ (x_0 - x_1 + x_2 - x_3)^2 &= b \\ (x_0 - x_1 - x_2 + x_3)^2 &= c \end{aligned}$$

und das Product

$$(3) \quad (x_0 + x_1 - x_2 - x_3)\,(x_0 - x_1 + x_2 - x_3)\,(x_0 - x_1 - x_2 + x_3) = r,$$

und ferner die Summe

(4) $$x_0 + x_1 + x_2 + x_3 = 4\,A$$

rationale Zahlen.

Wenn wir aus (2) die Quadratwurzeln ausziehen und berücksichtigen, dass sich $\sqrt{a}$ nach (3) von $\sqrt{b\,c}$ nur durch einen rationalen Factor unterscheidet, so folgt durch Addition:

(5) $$x_0 = A + B\sqrt{b} + C\sqrt{c} + D\sqrt{b\,c},$$

worin A, B, C, D rationale Zahlen sind; und daraus erhält man x_1, x_2, x_3, wenn man die Vorzeichen von $\sqrt{b}$, $\sqrt{c}$ ändert.

Nach Band I, §. 171 können aber alle Quadratwurzeln, nöthigenfalls unter Zuziehung von i, was ja selbst eine Kreistheilungszahl ist, rational durch die Kreistheilungsperioden (die Gauss'schen Summen) ausgedrückt werden, so dass also in (5) schon der Beweis unseres Satzes liegt.

Ist die Gruppe der biquadratischen Gleichung cyklisch, so können wir die Wurzeln so anordnen, dass die Gruppe aus den Permutationen

(6) $$1,\quad (0, 1, 2, 3),\quad (0, 2)\,(1, 3),\quad (0, 3, 2, 1)$$

besteht, und dann ist zu setzen:

(7) $$\begin{aligned} 4\,A &= x_0 + x_1 + x_2 + x_3 \\ (i, x_0) &= x_0 + i\,x_1 - x_2 - i\,x_3 \\ (-1, x_0) &= x_0 - x_1 + x_2 - x_3 \\ (-i, x_0) &= x_0 - i\,x_1 - x_2 + i\,x_3; \end{aligned}$$

darin ist A und $(-1, x_0)^2 = m$ rational, und daher kann $(-1, x_0)$ durch Kreistheilungszahlen ausgedrückt werden. Die vierten Potenzen

(8) $$(i, x_0)^4 = a + b\,i,\quad (-i, x_0)^4 = a - b\,i$$

sind Zahlen des Körpers $R(i)$, und um dieselben Schlüsse wie bei den cubischen Gleichungen ziehen zu können, kommt es also nur noch darauf an, $a + b\,i$ und $a - b\,i$ als vierte Potenzen von Kreistheilungszahlen darzustellen. Dazu dient noch der Satz, dass

(9) $$(i, x_0)\,(-i, x_0) = c$$

eine rationale Zahl ist.

Im Körper $R(i)$ haben wir (Bd. I, §. 173) die Einheiten ± 1, $\pm i$, ferner als Primzahlen die associirten Factoren $1 \pm i$ von 2, die reellen Primzahlen q der Form $4N + 3$ und die beiden complexen Factoren π, π' der reellen Primzahlen p von der Form $4N + 1$.

In Band I, §. 172 haben wir die Zerlegung

$$p = \psi_1(i)\, \psi_1(-i)$$

gefunden, die uns erlaubt,

$$\pi = \psi_1(i), \quad \pi' = \psi_1(-i) \tag{10}$$

zu setzen, und, wenn η eine N-gliedrige Periode von p^{ten} Einheitswurzeln ist,

$$(i, \eta)^4 = p\, \psi_1(i)^2, \quad (-i, \eta)^4 = p\, \psi_1(-i)^2,$$

oder

$$(i,\eta)^4 = \pi^3 \pi', \; (-i,\eta)^4 = \pi \pi'^3, \; (i,\eta)\,(-i,\eta) = p. \tag{11}$$

Zerlegen wir nun, wie bei den cubischen Gleichungen, die Zahlen $a + bi$, $a - bi$ in ihre Primfactoren in $R(i)$, so ergiebt sich unter Anwendung einer entsprechenden Bezeichnung

$$\begin{aligned} a + bi &= i^{\lambda}\; (1+i)^n\, q_1^{s_1}\, q_2^{s_2} \dots \pi_1^{t_1}\, \pi_1'^{t_1'}\, \pi_2^{t_2}\, \pi_2'^{t_2'} \dots \\ a - bi &= i^{-\lambda} (1-i)^n\, q_1^{s_1}\, q_2^{s_2} \dots \pi_1^{t_1'}\, \pi_1'^{t_1}\, \pi_2^{t_2'}\, \pi_2'^{t_2} \dots \end{aligned} \tag{12}$$

Das Product dieser beiden Zahlen muss aber die vierte Potenz einer rationalen Zahl sein [nach (8) und (9)], und daraus folgt:

$$\begin{aligned} n &\equiv 0 && && \pmod 4 \\ s_1 &\equiv 0, & s_2 &\equiv 0 \dots && \pmod 2 \\ t_1 + t_1' &\equiv 0, & t_2 + t_2' &\equiv 0 \dots && \pmod 4 \\ t_1 - t_1' &\equiv 0, & t_2 - t_2' &\equiv 0 \dots && \pmod 2. \end{aligned} \tag{13}$$

Es folgt aber jetzt aus (11):

$$\pi^t \pi'^{t'} = (\pi^3 \pi')^{\frac{t-t'}{2}}\, (\pi \pi')^{\frac{-t+3t'}{2}} = (i,\eta)^{2(t-t')}\, p^{\frac{-t+3t'}{2}}, \tag{14}$$

und ferner

$$(1 + i)^n = (-1)^{\frac{n}{4}}\, 2^{\frac{n}{2}}, \tag{15}$$

und hiernach können wir also, mit Rücksicht auf (13), wenn wir mit H_1, H_2 zwei Kreistheilungszahlen, nämlich das Product aller in der Zerlegung von $a + bi$ vorkommenden Zahlen

$$(i, \eta)^{\frac{t-t'}{2}},$$

und die durch die Vertauschung von i mit $-i$ daraus hervorgehende Zahl, ferner mit c eine rationale Zahl bezeichnen, setzen

$$\begin{aligned} a + bi &= i^{\lambda} \; c^2 H_1^4 \\ a - bi &= i^{-\lambda} c^2 H_2^4. \end{aligned}$$

Aus (8) folgt durch Ausziehen der 4ten Wurzel, wodurch eine Potenz von i als Factor hinzukommen kann,

$$(15) \qquad \begin{aligned} (i, x_0) &= i^h \sqrt[4]{i^{\lambda}} \sqrt{c}\, H_1 \\ (-i, x_0) &= i^{-h} \sqrt[4]{-i^{\lambda}} \sqrt{c}\, H_2 \\ (-1, x_0) &= \sqrt{m}, \end{aligned}$$

und daraus ergiebt sich, da $\sqrt[4]{i}$, $\sqrt{c}$ und $\sqrt{m}$ Kreistheilungszahlen sind, die Richtigkeit unseres Satzes auch in diesem Falle.

Auch hier kann die weitere Betrachtung des Baues der in (15) vorkommenden Ausdrücke dazu dienen, die Zusammensetzung der x_0, x_1, x_2, x_3 durch die Perioden η näher zu erforschen, was aber wieder zu keinen anderen Resultaten führen kann, als zu den schon in §. 24 abgeleiteten.

Wir haben also hiermit den Satz allgemein bewiesen, dass alle Abel'schen Körper dritten und vierten Grades Kreistheilungskörper sind, und dass alle diese Körper rational durch die Kreistheilungsperioden dargestellt werden können.

Fünfter Abschnitt.

Constitution der allgemeinen Gruppen.

§. 27.

Bildung von Gruppen nach Cayley.

Die allgemeine Definition der Gruppe, die im §. 1 gegeben ist, lässt über die Natur dieses Begriffes noch manches im Dunkel, und auch die verschiedenen einzelnen Gruppen, die wir im Verlauf unserer Betrachtungen kennen gelernt haben, geben nur Hinweise auf allgemeine Gesetze, und zeigen, dass der Gruppenbegriff an sich nichts Widersprechendes hat. In der Definition der Gruppe ist mehr enthalten, als es auf den ersten Blick den Anschein hat, und die Zahl der möglichen Gruppen, die aus einer gegebenen Anzahl von Elementen zusammengesetzt werden können, ist eine sehr beschränkte. Die allgemeinen Gesetze, die hier herrschen, sind erst zum kleinsten Theile erkannt, so dass jede neue specielle Gruppe, namentlich bei kleinerer Gliederzahl, ein neues Interesse bietet und zu eingehendem Studium auffordert.

Welche Gruppen sind zwischen einer gegebenen Zahl von Elementen, d. h. bei gegebenem Grade überhaupt möglich? Das ist die allgemeine Frage, um die es sich handelt, von deren vollständiger Lösung wir aber noch weit entfernt sind. Cayley hat diese Aufgabe zuerst für die niedrigsten Gradzahlen in Angriff genommen[1]).

---

[1]) On the theory of groups, as depending on the symbolic equation $\theta^n = 1$. Philosophical Magazine, Vol. II, 1854. (Cayley's mathematical papers, Vol. II, 125.) American Journal of mathematics, Vol. I.

Für jede beliebige Gradzahl n haben wir immer eine, nämlich die cyklische Gruppe, die wir erhalten, wenn wir $a^n = 1$ und die n Elemente

$$1, a, a^2 \dots a^{n-1}$$

als verschieden annehmen.

Wenn n eine Primzahl ist, so ist diese die einzige Gruppe vom Grade n (wenn isomorphe Gruppen als identisch betrachtet werden). Denn der Grad eines jeden Elementes einer Gruppe ist ein Theiler des Grades der Gruppe, und also hat in einer Gruppe von Primzahlgrad jedes Element, mit Ausnahme des Einheitselementes, den Grad n.

Um eine Gruppe vom Grade n vollständig darzustellen, müsste man eine quadratische Tafel construiren mit n^2 Feldern, die in n Zeilen und n Colonnen angeordnet sind. Man bezeichnet jede Zeile und jede Colonne durch eines der gegebenen Elemente, und setzt in das Feld, in dem diese beiden sich schneiden, das zusammengesetzte Element, wobei etwa der Zeilenzeiger die erste, der Colonnenzeiger die zweite Componente bedeutet:

	1	α	β	$\gamma \dots$
1	1	α	β	$\gamma \dots$
α	α	α^2	$\alpha\beta$	$\alpha\gamma \dots$
β	β	$\beta\alpha$	β^2	$\beta\gamma \dots$
γ	γ	$\gamma\alpha$	$\gamma\beta$	$\gamma^2 \dots$
. . .	. . .	. . .	. . .	. . .

Man kann aber die Felder einer solchen Tafel nicht ganz beliebig mit den Elementen ausfüllen, sondern man muss sich dabei an das associative Gesetz halten, so dass man, wenn man $\alpha\beta\gamma$ aufsucht, indem man zuerst in der Zeile α und in der Colonne β das Element $(\alpha\beta)$, dann in der Zeile $(\alpha\beta)$ und der Colonne γ das Element $(\alpha\beta)\gamma$ aufsucht, dasselbe Resultat findet, wie wenn man zuerst $(\beta\gamma)$ in der Zeile β und der Colonne γ und dann $\alpha(\beta\gamma)$ in der Zeile α und in der Colonne $(\beta\gamma)$ aufsucht.

Für $n = 4$ haben wir, wenn ein Element vom 4ten Grade existirt, die cyklische Gruppe

$$1, \alpha, \alpha^2, \alpha^3,$$

und wenn alle Elemente vom 1sten oder 2ten Grade sind, die Gruppen

$$1, \alpha, \beta, \alpha\beta$$

mit der Bedingung $\alpha\beta = \beta\alpha$. Es giebt also nur diese zwei Gruppen vom 4ten Grade. Wenn die Elemente mit 1, α, β, γ bezeichnet werden, so haben wir die beiden Tabellen:

	1	α	β	γ
1	1	α	β	γ
α	α	β	γ	1
β	β	γ	1	α
γ	γ	1	α	β

	1	α	β	γ
1	1	α	β	γ
α	α	1	γ	β
β	β	γ	1	α
γ	γ	β	α	1

Der Fall $n = 6$ lässt sich in folgender Weise vollständig erledigen: Wir bezeichnen die sechs Elemente mit 1, α, β, γ, δ, ε, so dass 1 die Einheit der Gruppe ist. Wenn darunter ein Element vom Grade 6 vorkommt, so ist die Gruppe cyklisch.

Wenn wir also von diesem Falle absehen, so können die Grade der Elemente α, β, γ, δ, ε nur 2 oder 3 sein. Sind α und β vom 2ten Grade, so kann $\alpha\beta$ nicht vom 2ten Grade sein; denn sonst wäre

$$\alpha = \alpha^{-1}, \quad \beta = \beta^{-1}, \quad \alpha\beta = \beta^{-1}\alpha^{-1} = \beta\alpha,$$

und es wäre also 1, α, β, $\alpha\beta$ eine Gruppe 4ten Grades; eine solche kann aber nicht Theiler einer Gruppe 6ten Grades sein.

Es muss also mindestens ein Element 3ten Grades vorkommen, und wenn wir ein solches mit α bezeichnen und γ nicht in 1, α, α^2 enthalten ist, so ordnet sich die Gruppe so:

$$(1) \qquad S = 1, \alpha, \alpha^2, \gamma, \gamma\alpha, \gamma\alpha^2.$$

Um die Bedingung zu ermitteln, dass dies eine Gruppe sei, bilden wir

$$\gamma S = \gamma, \gamma\alpha, \gamma\alpha^2, \gamma^2, \gamma^2\alpha, \gamma^2\alpha^2,$$

was mit S identisch sein muss; und es muss also

$$\gamma^2 = 1 \text{ oder } = \alpha \text{ oder } = \alpha^2$$

sein. Ist aber $\gamma^2 = \alpha$ oder $= \alpha^2$, so ist $\gamma^3 = \alpha\gamma$ oder $= \alpha^2\gamma$, und γ^6, aber keine niedrigere Potenz von $\gamma = 1$, d. h. S ist

cyklisch ($S = 1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5$). Es bleibt also nur die Annahme, dass γ vom 2ten Grade, also

$$(2) \qquad \gamma^2 = 1$$

ist. Da wir aber γ durch $\gamma\alpha$ oder $\gamma\alpha^2$ ersetzen können, so müssen auch diese vom 2ten Grade sein und es folgt:

$$(3) \qquad \gamma\alpha = \alpha^2\gamma, \quad \gamma\alpha^2 = \alpha\gamma,$$

mit deren Hülfe man jedes Compositum aus beliebig vielen Potenzen von α und γ immer auf eines und nur eines der Elemente S zurückführen kann. Und wenn man jetzt

$$1, \alpha, \alpha^2, \gamma, \gamma\alpha, \gamma\alpha^2$$

mit

$$1, \alpha, \beta, \gamma, \delta, \varepsilon$$

bezeichnet, so erhält man folgende Tabelle:

	1	α	β	γ	δ	ε
1	1	α	β	γ	δ	ε
α	α	β	1	ε	γ	δ
β	β	1	α	δ	ε	γ
γ	γ	δ	ε	1	α	β
δ	δ	ε	γ	β	1	α
ε	ε	γ	δ	α	β	1

Es kommen, wie es sein muss, in jeder Zeile und in jeder Colonne alle Elemente vor.

§. 28.

Beziehung der allgemeinen Gruppen zu den Permutationsgruppen.

Die Gruppen, die wir bisher am meisten angewandt haben, sind die Permutationsgruppen; diese Art von Gruppen gewinnen eine erhöhte Bedeutung auch für die allgemeine Gruppentheorie durch die folgenden Betrachtungen.

Es sei

$$(1) \qquad P = a_0, a_1, a_2, \ldots, a_{n-1}$$

eine beliebige Gruppe vom Grade n. Greifen wir aus P irgend

ein Element b heraus, so ist der Complex Pb mit P völlig identisch. Es können sich also die beiden Reihen

$$\begin{aligned} A &= a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1} \\ Ab &= a_0 b,\ a_1 b,\ a_2 b,\ \ldots,\ a_{n-1} b \end{aligned}$$

nur durch die Anordnung von einander unterscheiden. Der Uebergang von A zu Ab ist also eine Permutation von n Ziffern $0, 1, 2 \ldots n-1$, und jedem Elemente b von P entspricht eine solche Permutation, die wir mit π_b bezeichnen wollen. Zwei verschiedenen Elementen b, c entsprechen immer zwei verschiedene Permutationen π_b, π_c, und dem Einheitselemente entspricht die identische Permutation. Setzen wir

$$\pi_b = (A, Ab), \quad \pi_c = (A, Ac),$$

so können wir π_c auch mit (Ab, Abc) bezeichnen, und daraus ergiebt sich

(2) $$\pi_b \pi_c = \pi_{bc},$$

d. h. die Permutationen π bilden eine mit P isomorphe Permutationsgruppe. Diese Permutationsgruppe ist transitiv, da z. B. das Element a_0 in jedes beliebige andere Element von P übergehen kann. Also haben wir den Satz:

1. Jede Gruppe vom Grade n ist isomorph mit einer transitiven Permutationsgruppe von n Ziffern.

Es giebt natürlich noch andere mit einer gegebenen Gruppe isomorphe Permutationsgruppen, und es wäre von besonderem Interesse, eine solche Gruppe mit möglichst geringer Ziffernzahl zu bilden. Diese Aufgabe kann bis jetzt nicht allgemein gelöst werden. Wir müssen uns hier mit wenigen Sätzen begnügen.

Wir nehmen an, es sei R irgend ein Divisor von P vom Index j, und bezeichnen die Elemente von R mit c, setzen ferner, indem wir P in ein System von Nebengruppen zerlegen,

(3) $$P = R + Rb_1 + Rb_2 + \cdots + Rb_{j-1}.$$

Ist dann a irgend ein Element von P, so werden die beiden Systeme

(4) $$\begin{aligned} B &= R,\ Rb_1,\ Rb_2,\ \ldots,\ Rb_{j-1} \\ Ba &= Ra,\ Rb_1 a,\ Rb_2 a,\ \ldots,\ Rb_{j-1} a, \end{aligned}$$

von der Reihenfolge abgesehen, übereinstimmen, und es entspricht also jedem Element a eine bestimmte Permutation π_a der j Ziffern $0, 1 \ldots j-1$, die wir mit

(5) $$\pi_a = (B, Ba)$$

bezeichnen können. Auch hier gilt das Gesetz

(6) $$\pi_a \pi_{a'} = \pi_{a a'},$$

wenn a' gleichfalls irgend ein Element aus P ist. Es ist noch die Frage, ob verschiedene Elemente a dieselbe Permutation π hervorrufen können. Wenn $\pi_a = \pi_{a'}$ ist, so folgt aus (6):

$$\pi_{a' a^{-1}} = 1,$$

und wenn wir also mit a_0 alle der Bedingung

(7) $$\pi_{a_0} = 1$$

genügenden Elemente bezeichnen, so ist $a' = a_0 a$, und es kommt darauf an, die Gesammtheit der Elemente a_0 zu ermitteln. Wenn aber

(8) $$R b a_0 = R b$$

sein soll, so muss

$$b a_0 = c b$$

oder

$$a_0 = b^{-1} c b$$

sein, d. h. a_0 muss der Gruppe $b^{-1} R b$ angehören, und dies ist auch hinreichend für das Bestehen von (8).

Daraus ergiebt sich, dass die der Bedingung (7) genügenden Elemente a_0 die ganze Gruppe R_0 erfüllen, die der Durchschnitt aller mit R conjugirten Theiler von P:

$$R,\ b_1^{-1} R b_1,\ b_2^{-1} R b_2, \ldots,\ b_{j-1}^{-1} R b_{j-1},$$

und, wie wir früher nachgewiesen haben, ein Normaltheiler von P ist.

Daraus ergiebt sich für den Fall, dass $R_0 = 1$ ist, der Satz:

2. Hat eine Gruppe P einen Theiler vom Index j, der mit seinen conjugirten Theilern ausser dem Einheitselemente kein Element gemein hat, so ist P (einstufig) isomorph mit einer transitiven Permutationsgruppe von j Ziffern.

Dass die Permutationsgruppe transitiv ist, sieht man aus (4), wo für a jedes der Elemente $b_1, b_2, \ldots, b_{j-1}$ gesetzt werden kann.

Der Satz 2. findet immer statt, wenn P eine einfache Gruppe und R ein echter Theiler von P ist, weil dann R_0, als Normaltheiler von P, sich auf die Einheitsgruppe reduciren muss[1]).

Es mögen jetzt R und Q irgend zwei Theiler der Gruppe P bedeuten, R vom Index j, Q vom Grade q.

---

[1]) Hölder, Mathematische Annalen, Bd. 40, S. 57.

Wir zerlegen P wie in (4) in die j Nebengruppen B, bezeichnen mit e alle Elemente von Q, und untersuchen nun die Permutation

$$\pi_e = (B, Be),$$

die durch die Elemente e unter den j Elementen (4) hervorgerufen wird. Diese Permutationen bilden nach (5) und (6) gewiss eine mit Q ein- oder mehrstufig isomorphe Gruppe Π.

Ist a_1 irgend ein Element von P, so werden in dem nach der Composition der Theile gebildeten Complex

$$P_1 = R a_1 Q$$

eine gewisse Anzahl der Nebengruppen B enthalten sein. Diese Anzahl finden wir, wenn wir die Bedingung aufsuchen, dass $R a_1 = R a_1 e$ sei, oder dass $a_1 e$ in $R a_1$ oder e in $a_1^{-1} R a_1$ enthalten sei. Ist also

$$Q_1 \text{ der Durchschnitt von } Q \text{ und } a_1^{-1} R a_1$$

vom Index h_1 in Bezug auf Q, so enthält P_1 genau h_1 und nicht mehr von den Complexen B.

Ist a_2 ein zweites Element von P, so ist der Complex

$$P_2 = R a_2 Q$$

entweder völlig mit P_1 übereinstimmend, oder beide enthalten gar kein gemeinsames Element. Denn wenn P_1 und P_2 ein gemeinsames Element enthalten, so haben sie einen der Complexe B gemein. Das ist aber nur möglich, wenn $a_2 e$ in $R a_1 e'$, also a_2 in P_1 enthalten ist, und dann ist P_1 und P_2 identisch. Wir können also mit der Bildung der Complexe $P_1, P_2 \ldots$ fortfahren, bis die Gruppe P erschöpft ist, und erhalten die Zerlegung der Gruppe P nach den zwei Gruppen Q und R:

$$(9) \qquad \begin{aligned} P &= R a_1 Q + R a_2 Q + \cdots \\ &= P_1 \quad\;\; + P_2 \quad\;\; + \cdots \end{aligned}$$

Aus der Bemerkung, dass, wenn a_2 nicht in $R a_1 Q$ vorkommt, a_2^{-1} nicht in $Q a_1^{-1} R$ enthalten ist, ergiebt sich die zweite Zerlegung:

$$(10) \qquad P = Q a_1^{-1} R + Q a_2^{-1} R + \cdots [1].$$

Die Bestandtheile $P_1, P_2, \ldots$ von (9) enthalten je $h_1, h_2, \ldots$ Elemente der Reihe B, wenn $h_1, h_2, \ldots$ die Indices der Durchschnitte von Q mit $a_1^{-1} R a_1$, $a_2^{-1} R a_1, \ldots$ in Bezug auf Q, also Theiler des Grades q von Q bedeuten.

---

[1]) Diese Zerlegungen verdanke ich einer Mittheilung von Dedekind.

Wenn nun e ein beliebiges Element aus Q ist, so ist $Qe = Q$, und folglich auch $Ra_i Qe = Ra_i Q$. Daraus folgt, dass durch Composition mit e die Gesammtheit der h_i Elemente, aus denen P_i zusammengesetzt ist, nicht geändert wird, und dass sie also durch die Permutationsgruppe Π nur unter einander vertauscht werden. Man sieht aber auch unmittelbar, dass diese h_i Elemente B durch Π transitiv verbunden sind; denn P_1 besteht eben aus allen den Complexen B, die aus einem unter ihnen durch Anwendung von Elementen aus Q abgeleitet werden können, und daher kann jeder dieser Complexe B aus P_i durch Permutationen aus Π in jeden anderen übergeführt werden.

Wir wollen das gewonnene Resultat in folgender Weise als Theorem formuliren:

3. Ist P eine Gruppe vom Grade n, R ein Theiler von P vom Index j, Q ein Theiler von P vom Grade q, so ist mit Q eine Permutationsgruppe Π von j Ziffern ein- oder mehrstufig isomorph. Die j Ziffern zerfallen in Reihen von je $h_1, h_2, h_3, \ldots$ durch Π transitiv verbundenen Ziffern, so dass

$$j = h_1 + h_2 + h_3 + \cdots \tag{11}$$

ist, und $h_1, h_2, h_3, \ldots$ Theiler von q sind. Die Zahlen $h_1, h_2, h_3, \ldots$ sind die Indices von Theilern von Q, die sich als Durchschnitte von Q mit den conjugirten Gruppen $a^{-1}Ra$ ergeben.

Haben die verschiedenen Gruppen $Q_1, Q_2, \ldots$ ausser dem Einheitselemente keinen gemeinschaftlichen Theiler, was bei einfachen Gruppen P immer eintritt, so ist der Isomorphismus einstufig.

§. 29.

Der erste Sylow'sche Satz.

Es ist nicht leicht, auf dem von Cayley eingeschlagenen directen Wege bei der Bildung von Gruppen über die niedrigsten Gradzahlen hinauszugehen. Für weitergehende Untersuchungen in dieser Richtung ist ein Satz von grossem Nutzen, der in beschränktem Umfange von Cauchy herrührt, allgemein aber von Sylow bewiesen ist. Wir wollen diesen wichtigen Satz

hier nach einem Verfahren von Frobenius beweisen, das sich nur auf den allgemeinen Gruppenbegriff stützt [1]).

Der Satz lässt sich einfach so aussprechen:

I. Ist P eine Gruppe von irgend welchen Elementen vom Grade n und $p^\varkappa$ eine in n aufgehende Primzahlpotenz, so hat die Gruppe P einen Theiler vom Grade $p^\varkappa$.

Cauchy hat diesen Satz für $\varkappa = 1$ bewiesen. Für den Fall, dass n eine Primzahl ist, ist er evident; für $n = 4$ und $n = 6$ kann man ihn aus den Zusammenstellungen in §. 27 leicht ablesen, so dass er also für die Fälle $n = 2, 3, 4, 5, 6, 7$ als erwiesen betrachtet werden kann. Auf Grund dieser Wahrnehmung lässt sich die vollständige Induction anwenden, und wir setzen also voraus, der Satz sei bewiesen für Gruppen, deren Grad niedriger ist als n.

Wir wollen die Elemente der Gruppe P durch die Buchstaben $a, b, c, \ldots$ bezeichnen und unter x ein Zeichen für ein veränderliches Element in P verstehen, das die ganze Gruppe P durchläuft.

Wir fassen zunächst alle die Elemente a zusammen, die der Bedingung

$$(1) \qquad x^{-1} a x = a \quad \text{oder} \quad a x = x a$$

genügen, so dass a jedes Element bedeutet, das mit allen Elementen von P vertauschbar ist. Dazu gehört jedenfalls das Einheitselement, und die Gesammtheit dieser Elemente a bildet eine in P enthaltene Gruppe A. Denn aus

$$x^{-1} a x = a, \quad x^{-1} a' x = a'$$

folgt

$$x^{-1} a a' x = a a'.$$

A ist eine Abel'sche Gruppe und ein Normaltheiler von P; denn aus der Definition (1) folgt $x^{-1} A x = A$, und für irgend zwei Elemente a, a' von A:

$$a a' = a' a.$$

Wir bezeichnen mit ν und j Grad und Index dieser Gruppe, so dass

$$(2) \qquad n = \nu j$$

---

[1]) Cauchy, Exerc. d'analyse, Tom. III. Sylow, Mathem. Annalen, Bd. 5. Frobenius, Journ. für Mathematik, Bd. 100. Netto, Mathem. Annalen, Bd. 13; Substitutionentheorie, §. 48.

ist. Wenn nun c ein nicht zu A gehöriges Element von P ist, so wird $x^{-1}cx$ nicht für alle Elemente x gleich c sein. Es werden sich aber gewisse Elemente $b, b', \dots$ unter den x finden, darunter gewiss das Einheitselement, die der Bedingung

$$x^{-1}cx = c$$

genügen, und diese Elemente bilden eine Gruppe, weil aus

(3) $$b^{-1}cb = c, \quad b'^{-1}cb' = c$$

folgt, dass auch

$$(b'b)^{-1}c(b'b) = b^{-1}b'^{-1}cb'b = c$$

sein muss. Diese Gruppe bezeichnen wir mit B und ihren Grad und Index mit μ, ε, so dass

(4) $$n = \mu\varepsilon$$

wird; B ist ein echter Theiler von P, und daher ist ε jedenfalls grösser als 1, weil sonst c in A enthalten wäre, gegen die Annahme.

Ist g ein Element von P, das nicht in B vorkommt, und b ein beliebiges Element von B, so ist nach (3):

(5) $$g^{-1}b^{-1}cbg = g^{-1}cg,$$

was von c verschieden ist, weil g nicht in B vorkommt. Wenn man also P in die Nebengruppen zerlegt:

(6) $$P = B + Bg_1 + Bg_2 + \cdots + Bg_{\varepsilon-1},$$

so erhält man, wenn man in $x^{-1}cx$ für x alle Elemente einer dieser Nebengruppen setzt, immer dasselbe Element $g^{-1}cg$, und man erhält also ε und nicht mehr Elemente, und jedes gleich oft:

(7) $$c, \; g_1^{-1}cg_1, \; g_2^{-1}cg_2, \; \dots, \; g_{\varepsilon-1}^{-1}cg_{\varepsilon-1};$$

alle diese Elemente, deren Gesammtheit wir mit C bezeichnen wollen, sind unter einander und von den Elementen a verschieden. C ist aber keine Gruppe, da das Einheitselement darunter nicht vorkommt.

Ist nun mit A und C die Gesammtheit der Elemente von P noch nicht erschöpft, so nehme man ein in A und C nicht vorkommendes Element c' und bilde nach derselben Vorschrift die Gruppe B' vom Grade μ' aller Elemente, die der Bedingung

$$b'^{-1}c'b' = c'$$

genügen, und das System C':

(8) $$c', \; g_1'^{-1}c'g_1', \; g_2'^{-1}c'g_2', \; \dots, \; g_{\varepsilon'-1}^{-1}c'g_{\varepsilon'-1},$$

und man sieht dann, dass diese Elemente alle von den Elementen C verschieden sind, da, wenn $g'^{-1}c'g' = g^{-1}cg$ wäre, auch $c' = g'g^{-1}cgg'^{-1}$ wäre, und es würde also gegen die Voraussetzung c' schon in C vorkommen. Auf diese Weise fährt man mit der Bildung der Gruppen $B, B', B'', \ldots$ und der Systeme $C, C', C'', \ldots$ fort, bis alle Elemente von P in den Systemen $A, C, C', C'', \ldots$ untergebracht sind. Man hat dann die Zahlengleichungen:

$$(9) \qquad n = \nu j = \mu\varepsilon = \mu'\varepsilon' = \mu''\varepsilon'' \ldots$$

$$(10) \qquad n = \nu + \varepsilon + \varepsilon' + \varepsilon'' + \cdots$$

Auf Grund dieser Formeln lässt sich nun der Sylow'sche Satz durch vollständige Induction beweisen, wobei zwei Fälle zu unterscheiden sind:

1) Der Grad ν von A ist durch p theilbar. In diesem Falle giebt es, weil A eine Abel'sche Gruppe ist, nach §. 9, 2. ein Element a in A vom Grade p, und die cyklische Gruppe p^{ten} Grades

$$1, a, a^2, \ldots, a^{p-1},$$

die wir mit Q bezeichnen, ist ein Normaltheiler von P, weil ja für ein Element a von A immer $x^{-1}ax = a$ sein sollte. Die complementäre Gruppe zu Q, P/Q ist vom Grade $n:p$, und ihr Grad ist also kleiner als n und durch $p^{\varkappa-1}$ theilbar. Nach unserer Voraussetzung giebt es also einen Theiler von P/Q vom Grade $p^{\varkappa-1}$, und folglich giebt es nach §. 6, 2. einen Theiler von P vom Grade $p^{\varkappa}$.

2) Der Grad ν von A ist nicht durch p theilbar. Da n durch p theilbar ist, so können in diesem Falle nach (10) nicht alle Zahlen $\varepsilon, \varepsilon', \varepsilon'', \ldots$, die alle grösser als 1 sind, durch p theilbar sein. Wenn nun ε nicht durch p theilbar ist, so ist μ durch $p^{\varkappa}$ theilbar. Der Grad der Gruppe B ist kleiner als n und durch $p^{\varkappa}$ theilbar, und also giebt es nach Voraussetzung einen Theiler von B, der also auch Theiler von P ist, vom Grade $p^{\varkappa}$.

Hiermit ist der Satz I bewiesen.

Zu diesem Satze kommen aber noch wesentliche Ergänzungen.

§. 30.

Der zweite Sylow'sche Satz.

Es sei nun, wie oben, P eine Gruppe vom Grade n und $p^\varkappa$ die höchste Potenz der Primzahl p, die in n aufgeht; Q sei ein Theiler von P vom Grade $p^\varkappa$, der nach dem Satze I, §. 29 existirt.

Der Inbegriff aller Elemente c von P, die der Bedingung genügen:

(1) $$c^{-1} Q c = Q,$$

unter denen gewiss alle Elemente von Q enthalten sind, bildet eine Gruppe; denn aus

$$Q c = c Q, \quad Q c' = c' Q$$

folgt, dass auch $Q c c' = c c' Q$ ist. Diese Elemente c können wir die mit der Gruppe Q vertauschbaren Elemente von P nennen. Bezeichnen wir die Gruppe der c mit R, so ist R ein Theiler von P, und Q ein Theiler von R, und zwar ein Normaltheiler. In besonderen Fällen kann R sowohl mit Q, als mit P identisch sein. Ist aber b irgend ein nicht in R enthaltenes Element von P, so giebt es unter den Elementen der Gruppe $b^{-1} Q b$ gewiss wenigstens eines, das nicht in Q enthalten ist.

Bezeichnen wir mit r den Index von Q in Bezug auf R, mit j den Index von R in Bezug auf P, so ist

(2) $$n = p^\varkappa r j,$$

und r und j sind durch p nicht theilbar.

Der Satz, den wir zu beweisen haben, lautet:

II. Der Index j von R ist von der Form $pk + 1$, worin k irgend eine ganze Zahl ist [$j \equiv 1 \pmod{p}$]; es giebt j und nicht mehr verschiedene Theiler von P vom Grade $p^\varkappa$, die alle mit einander conjugirt sind. Jeder Theiler von P, dessen Grad eine Potenz von p ist, ist in einer dieser conjugirten Gruppen enthalten.

Ist c ein Element aus R vom Grade γ, und s der kleinste positive Exponent, für den c^s in Q enthalten ist, so muss jeder andere Exponent t, für den c^t zu Q gehört, durch s theilbar

sein. Denn setzen wir $t = ms + s_1$, worin $s_1 < s$ ist, so ist c^{s_1} in Q enthalten, und s_1 muss also $= 0$ sein. Demnach ist s ein Theiler von γ. Nun bilden aber die Elemente

$$Q + cQ + c^2 Q + \cdots c^{s-1} Q$$

wegen (1) eine in P enthaltene Gruppe, und zwar vom Grade $p^x s$, und da also $p^x s$ ein Theiler von n sein muss, so folgt, dass s nicht durch p theilbar sein kann. Wäre nun der Grad γ von c eine Potenz von p, so müsste auch s eine Potenz von p sein, was hiernach nicht möglich ist.

Es kann also der Grad von c gewiss nicht eine Potenz von p sein; d. h. ausser den Elementen Q giebt es in R keine Elemente, deren Grad eine Potenz von p ist.

Bedeutet nun b ein Element von P, das nicht zu R gehört, so giebt es nach der Definition von R in der Gruppe

$$Q' = b^{-1} Q b$$

mindestens ein Element, das nicht in Q vorkommt, und der Grad dieses Elementes muss eine Potenz von p sein, weil der Grad von Q' gleich p^x, also eine Potenz von p ist. Dies Element kann also nicht in R vorkommen, und Q' ist daher kein Theiler von R.

Wählen wir die Elemente $b_1, b_2, \ldots, b_{j-1}$ aus P so aus, dass wir

(10) $$P = R + Rb_1 + Rb_2 + \cdots + Rb_{j-1}$$

setzen können, so sind also die $j - 1$ Gruppen:

$$b_1^{-1} Q b_1, \quad b_2^{-1} Q b_2, \ldots, b_{j-1}^{-1} Q b_{j-1},$$

die alle vom Grade p^x sind, von Q verschieden. Sie sind aber auch von einander verschieden; denn wäre z. B.

$$b_1^{-1} Q b_1 = b_2^{-1} Q b_2,$$

so würde folgen:

$$b_2 b_1^{-1} Q b_1 b_2^{-1} = Q,$$

d. h. $b_2 b_1^{-1} = c$ wäre in R enthalten, also $b_2 = cb_1$ in Rb_1, was wegen (10) nicht möglich ist. Wir haben also gewiss j verschiedene conjugirte Gruppen $p^{x\text{ten}}$ Grades:

(11) $$Q, \; b_1^{-1} Q b_1, \; b_2^{-1} Q b_2, \ldots, b_{j-1}^{-1} Q b_{j-1}.$$

Ist $Q' = b^{-1} Q b$ eine von ihnen, so enthält $R' = b^{-1} R b$ den Theiler Q', aber ausser diesem kein Element, dessen Grad

eine Potenz von p ist. R' ist der Inbegriff aller mit Q' vertauschbaren Elemente von P.

Wir wenden nun weiter den Satz 3., §. 28 an, indem wir unter P, R, Q die Gruppen verstehen, die hier mit denselben Buchstaben bezeichnet sind. Da hier Q ein Theiler von R ist, so ist $h_1 = 1$. Von den conjugirten Gruppen $b^{-1}Rb$ ist aber keine ausser R durch Q theilbar, und also sind die übrigen $h_2, h_3, \ldots$ alle grösser als 1. Sie sind aber, da sie Theiler des Grades von Q sein müssen, Potenzen von p und aus der Gleichung

$$j = h_1 + h_2 + h_3 + \cdots$$

folgt also $j \equiv 1 \pmod p$.

Ist aber Q_1 irgend ein Divisor von P, dessen Grad eine Potenz von p ist, so wenden wir wieder die Zerlegung von j nach dem Theorem 3., §. 28 an, indem wir für die dort vorkommenden Gruppen P, R, Q die Gruppen P, R, Q_1 setzen. Dann ist wieder

$$j = h_1 + h_2 + h_3 + \cdots,$$

worin jetzt $h_1, h_2, h_3, \ldots$ die Indices (in Bezug auf Q) der Durchschnitte von Q_1 mit der Gruppe R und seinen conjugirten bedeuten, die also auch Potenzen von p sind. Da aber $j \equiv 1 \pmod p$ ist, so muss mindestens eine von den Zahlen $h = 1$ sein, d. h. eine der Gruppen $b_\lambda^{-1} R b_\lambda$ und folglich auch eine der Gruppen (11) ist durch Q_1 theilbar. Ist Q_1 vom Grade $p^\varkappa$, so ist es mit einer der Gruppen (11) identisch.

Damit ist also das Theorem II vollständig bewiesen.

§. 31.

Gruppen vom Grade p^α.

Sylow hat aus seinen Sätzen eine merkwürdige Eigenschaft der Gruppen abgeleitet, deren Grad eine Potenz einer Primzahl p, p^α, ist. Es sei also P eine solche Gruppe und β eine positive Zahl, kleiner als α. Dann enthält nach dem Satze I, §. 29 die Gruppe P einen Theiler Q vom Grade p^β, deren Index $p^{\alpha-\beta}$ ist. Wir wenden den Satz 3., §. 28 an, indem wir für R und Q diese Gruppe Q vom Grade p^β setzen, dann sind $h_1, h_2, h_3, \ldots$

die Indices von Q und den mit Q conjugirten Theilern von P in Bezug auf Q. Daher ist $h_1 = 1$ und

$$p^{\alpha-\beta} = h_1 + h_2 + h_3 \ldots$$

Die Summanden $h_1, h_2, h_3, \ldots$ können hier als Theiler des Grades von Q nur Potenzen von p sein, und da $h_1 = 1$ ist, so folgt, dass mindestens p dieser Summanden $= 1$ sein müssen, da sonst ihre Summe nicht durch p theilbar sein könnte. Das heisst aber nichts Anderes, als dass wenigstens $p - 1$ der conjugirten Gruppen $b^{-1}\,Q\,b$, wo b nicht in Q enthalten ist, durch Q theilbar und also gleich Q sein müssen. Wenn aber

$$b^{-1}\,Q\,b = Q$$

ist, so ist auch für jeden Exponenten s

$$b^{-s}\,Q\,b^{s} = Q.$$

Ist b^r die niedrigste Potenz von b, die in Q enthalten ist, so muss, da der Grad von b eine Potenz von p ist, auch r eine Potenz von p sein, und

$$b^{\frac{r}{p}} = c$$

ist ein Element von P, das selbst nicht in Q vorkommt, dessen p^{te} Potenz aber in Q enthalten ist, und das zugleich der Bedingung

$$c\,Q\,c^{-1} = Q$$

genügt. Daraus folgt, dass die Elemente

$$R = Q + Qc + Qc^2 + \cdots + Qc^{p-1}$$

eine Gruppe vom Grade $p^{\beta+1}$ bilden, von der Q ein Normaltheiler ist. Wir haben also den Satz:

III. Ist P eine Gruppe vom Grade p^α und Q ein Theiler von P vom Grade p^β $(\beta < \alpha)$, so giebt es einen Theiler R von P vom Grade $p^{\beta+1}$, von dem Q Normaltheiler ist.

Nimmt man in diesem Satze $\beta = \alpha - 1$ an, so fällt R mit P zusammen, und es ergiebt sich, dass Q ein Normaltheiler von P ist. Wendet man denselben Satz auf die Gruppe Q an u. s. f., so erhält man:

IV. Jede Gruppe, deren Grad eine Primzahlpotenz ist, ist metacyklisch (§. 8).

§. 32.

Satz von Frobenius.

Frobenius hat einen Satz aufgestellt, der als ein Gegenstück zum vierten Sylow'schen betrachtet werden kann, der sich so aussprechen lässt[1]):

V. Jede Gruppe, deren Grad ein Product von lauter verschiedenen Primzahlen ist, ist metacyklisch.

Wir setzen also voraus, dass der Grad n einer Gruppe P durch keine Quadratzahl theilbar sei. Ist t der grösste Primtheiler von n, so giebt es nach dem Cauchy-Sylow'schen Satze (§. 29) einen Theiler T vom Grade t von P, der, weil t eine Primzahl ist, eine cyklische Gruppe ist, also aus den Elementen

$$T = 1, a, a^2, \dots a^{t-1}$$

besteht. Wenn sich nun nachweisen liesse, dass unter den gemachten Voraussetzungen T ein Normaltheiler von P ist, so könnte man dieselbe Schlussweise auf die Gruppe P/T, deren Grad $n:t$ ist, anwenden, und würde, wenn t_1 die zweitgrösste in n aufgehende Primzahl ist, auf einen Normaltheiler N der Gruppe P/T vom Grade t_1 schliessen. Daraus würde dann aber folgen (§. 6, 2.), dass P einen Normaltheiler T_1 vom Grade $t\,t_1$ hat, von dem T selbst wieder Normaltheiler ist. Indem man in gleicher Weise die Gruppe P/T_1 betrachtet u. s. f., ergiebt sich eine Compositionsreihe von P:

$$P, T_k, T_{k-1}, \dots T_1, T, 1,$$

in der die Indexreihe aus den der Grösse nach aufsteigend geordneten Primfactoren von n besteht, und P ergiebt sich als metacyklisch. Alles kommt also darauf an, nachzuweisen, dass T ein Normaltheiler von P ist.

Dieser Satz ist leichter zu beweisen, wenn man ihn als speciellen Fall eines allgemeineren betrachtet, als wenn man ihn direct angreift. Dieser allgemeinere Satz lautet unter den über P und n gemachten Voraussetzungen:

α) Ist $n = \mu\,\nu$ in zwei Factoren zerlegt und ist jeder Primtheiler von ν grösser als jeder Prim-

---

1) Frobenius, Sitzungsberichte der Berl. Akademie, 4. Mai 1893.

theiler von μ, so giebt es ν und nicht mehr Elemente in P, deren Grad in ν aufgeht.

Wenden wir diesen Satz auf $\nu = t$ an, so folgt, dass es ausser T keine Elemente in P geben kann, deren Grad $= t$ ist. Wenn aber c irgend ein Element von P ist, so ist die mit T conjugirte Gruppe $c^{-1} T c$ gleichfalls vom Grade t, und muss also mit T identisch sein. Damit ist dann bewiesen, dass T ein Normaltheiler von P ist.

Zum Beweis des Satzes α) wendet man die vollständige Induction an. Derselbe ist offenbar richtig, wenn $\mu = 1$, $\nu = n$ ist, und wir setzen also als bewiesen voraus:

α') Ist $\mu' \nu'$ durch kein Quadrat theilbar, jeder Primtheiler von ν' grösser als jeder Primtheiler von μ', und die Anzahl der Primtheiler von μ' kleiner als die Anzahl der Primtheiler von μ, so giebt es in jeder Gruppe vom Grade $\mu' \nu'$ genau ν' Elemente, deren Grad ein Theiler von ν' ist.

Um daraus den Beweis des Satzes α) abzuleiten, bezeichnen wir mit p den grössten Primtheiler von μ und mit Q eine in P enthaltene Gruppe vom Grade p, deren Existenz nach dem Cauchy-Sylow'schen Theorem feststeht. Dann sind alle Primfactoren von ν grösser als p. Wie in §. 30 bezeichnen wir mit R die Gruppe, die aus allen der Bedingung

$$c^{-1} Q c = Q$$

genügenden Elementen c von P besteht, deren Grad wir, wie oben, mit pr bezeichnen; j bedeutet, wie früher, den Index des Theilers R von P. Wir setzen $r = r_1 r_2$, und verstehen unter r_1 den grössten gemeinschaftlichen Theiler von μ und r, so dass r_2 der grösste gemeinschaftliche Theiler von ν und r ist. Es ist dann

$$n = \mu \nu = r_1 p r_2 j.$$

Nach der Hypothese α') enthält nun P genau $p\nu$ Elemente, deren Grad ein Theiler von $p\nu$ ist; es möge mit U die Gesammtheit dieser Elemente bezeichnet sein. Die Gruppe R enthält aber, gleichfalls nach α'), genau $p r_2$ Elemente, deren Grad ein Theiler von $p r_2$, also ein Theiler von $p\nu$ ist. Dieses System wollen wir mit V bezeichnen. Offenbar sind alle Elemente von V zugleich in U enthalten.

Wenn wir nun noch beweisen können, dass es in U genau $(p-1)\nu$ Elemente giebt, deren Grad durch p theilbar ist, so sind wir am Ziele; denn dann folgt, dass es unter den Elementen U und also auch unter den Elementen von P genau

$$p\nu - (p-1)\nu = \nu$$

giebt, deren Grad ein Theiler von ν ist.

Dies ergiebt sich aber aus Folgendem:

β) Ist v ein Element aus V, so gehören alle Elemente vQ (deren Anzahl p beträgt) zu V. Es giebt darunter $p-1$, deren Grad durch p theilbar ist, und eines, dessen Grad nicht durch p theilbar ist. In V giebt es $(p-1)\,r_2$ Elemente, deren Grad durch p theilbar ist, und r_2 Elemente, deren Grad nicht durch p theilbar ist.

Denn ist a ein von 1 verschiedenes Element von Q, so ist, da v zu R gehört, also $v^{-1}av$ in Q enthalten ist, und da Q aus den Potenzen von a besteht,

(1) $$v^{-1}av = a^s.$$

Durch wiederholte Anwendung ergiebt sich daraus für jeden Exponenten h

(2) $$v^{-h}av^h = a^{s^h}.$$

Nehmen wir für h den Grad des Elementes v, der nach der Voraussetzung ein Theiler von $p\nu$ ist, setzen also $v^h = 1$, so folgt

(3) $$a = a^{s^h}, \quad s^h \equiv 1 \pmod{p}.$$

In h gehen aber keine anderen Primfactoren auf als solche, die gleich oder grösser als p sind, und also ist $p-1$ relativ prim zu h und man kann der Congruenz

(4) $$xh \equiv 1 \pmod{p-1}$$

genügen; demnach ergiebt sich aus dem Fermat'schen Lehrsatze:

(5) $$s^{xh} \equiv s \equiv 1 \pmod{p},$$

also nach (1):

(6) $$av = va,$$

d. h. a und v sind vertauschbar. Daraus folgt für jeden Exponenten λ

(7) $$(va)^\lambda = v^\lambda a^\lambda.$$

Ist, wie vorhin, h der Grad von v, und setzen wir, wenn h durch p theilbar ist, $\lambda = h$, und wenn h nicht durch p theilbar ist, $\lambda = hp$, so folgt aus (7) $(va)^\lambda = 1$, d. h. der Grad von va ist ein Theiler von h oder von hp, also jedenfalls ein Theiler von pv; d. h. va ist in V enthalten.

Ersetzen wir nun in (7) a durch a^x und lassen x die Reihe der Zahlen $0, 1, \ldots p - 1$ durchlaufen, so durchläuft a^x die Gruppe Q und va^x das System vQ, und es ist für jedes λ

(8) $$(va^x)^\lambda = v^\lambda a^{x\lambda}.$$

Wenn nun der Grad h von v nicht durch p theilbar ist, so ist

$$(va^x)^h = a^{xh},$$

also nur dann $= 1$, wenn $x = 0$ ist; dagegen ist

$$(va^x)^{ph} = 1,$$

d. h. der Grad von va^x ist, wenn x nicht $= 0$ ist, ein Theiler von ph, aber nicht von h, also durch p theilbar; dagegen ist er $= h$, wenn $x = 0$ ist.

Ist aber der Grad h von v durch p theilbar, so ist er von der Form pg, und g ist durch p nicht theilbar, weil p nur einfach in n, also auch in h aufgeht. Es ist also v^g ein Element aus R vom Grade p, und muss also nach §. 30 in Q enthalten sein. Setzen wir also hiernach

$$v^g = a^y,$$

so wird

$$(va^x)^g = a^{y+gx},$$

und dies ist dann und nur dann $= 1$, wenn $y + gx \equiv 0 \pmod{p}$ wird, was nur für einen Werth von x eintritt. Für diesen Werth von x ist der Grad von va^x ein Theiler von g; für die anderen Werthe von x ist er Theiler von pg, aber nicht von g, also durch p theilbar. Damit sind die beiden ersten Behauptungen des Satzes β) erwiesen.

Um auch den letzten Theil einzusehen, bemerke man, dass, wenn v_1, v_2 zwei Elemente aus V bedeuten, die Systeme $v_1 Q$, $v_2 Q$ entweder ganz identisch sind, oder kein einziges gemeinschaftliches Element haben. Daraus folgt, dass man V in der Weise darstellen kann:

$$V = v_1 Q + v_2 Q + \cdots + v_{r_2} Q$$

(obwohl V im Allgemeinen keine Gruppe ist), und in jedem dieser r_2 Theilsysteme vQ giebt es $p - 1$ Elemente, deren Grad

durch p theilbar ist, und ein Element, dessen Grad nicht durch p theilbar ist.

Nach dem Satze II, §. 30 giebt es j und nicht mehr von einander verschiedene conjugirte Gruppen $Q, Q', Q'', \ldots Q^{(j-1)}$ in P, und j von einander verschiedene conjugirte Gruppen $R, R', R'', \ldots R^{(j-1)}$.

Es lässt sich hiernach der Satz beweisen:

γ) Jedes Element von P, dessen Grad durch p theilbar ist, kommt in einer und nur in einer der Gruppen $R, R', R'' \ldots R^{(j-1)}$ vor.

Die Gruppen $Q, Q', Q'' \ldots$ sind, da ihr Grad eine Primzahl ist, cyklisch, und je zwei enthalten, weil sie von einander verschieden sind, ausser dem Einheitselemente kein gemeinsames Element. Es sei

$$Q = 1, a, a^2, \ldots a^{p-1}.$$

Die Gruppe R, die aus allen der Bedingung

$$c^{-1} Q c = Q$$

genügenden Elementen besteht, enthält ausser den Potenzen von a kein Element vom Grade p; und Entsprechendes gilt für die anderen Gruppen $Q', R', Q'', R'' \ldots$

Ist nun b ein Element von P, dessen Grad durch p theilbar ist und gleich ps sein mag, so dass s nicht durch p theilbar ist, so ist b^s ein Element, dessen Grad p ist, und das also in einer und nur in einer der cyklischen Gruppen $Q, Q', Q'' \ldots$ vorkommt. Ist aber $b^s = a$ ein Element von Q, so ist

$$b^{-1} a b = a,$$

d. h. b kommt in der Gruppe R vor, und kann in keiner der anderen Gruppen, z. B. in R', vorkommen, weil sonst b^s auch in Q' vorkäme, was nicht möglich ist, da Q und Q' nur das Einheitselement gemein haben. Damit ist γ) bewiesen.

δ) In U giebt es genau $j r_2 (p-1)$ Elemente, deren Grad durch p theilbar ist.

Unter U haben wir die Gesammtheit der Elemente von P verstanden, deren Grad ein Theiler von pr ist. Nun giebt es nach β) in R genau $r_2 (p-1)$ Elemente aus U, deren Grad durch p theilbar ist, und da jede der j Gruppen $R, R', R'' \ldots$ an Stelle von R treten kann, so folgt δ) aus γ). Um also noch zu zeigen, worauf nach dem Obigen alles ankommt, dass in U

genau $(p-1)\nu$ Elemente vorkommen, deren Grad durch p theilbar ist, ist also nur noch die Formel

$$\varepsilon) \quad \nu = j r_2$$

zu beweisen. Diese ergiebt sich aus folgender Ueberlegung. Nach α') ist die Anzahl der Elemente U gleich $p\nu$. Unter diesen Elementen U ist aber gewiss eines, das Einheitselement, dessen Grad nicht durch p theilbar ist, und folglich ist nach δ)

$$j r_2 (p-1) < p\nu.$$

Andererseits ist $n = \mu\nu = p r_1 r_2 j$, und da ν relativ prim zu $p r_1$ ist, so ist $j r_2$ durch ν theilbar. Also ist $j r_2 : \nu$ eine ganze positive Zahl, die kleiner als $p : p-1$ und folglich auch kleiner als 2 ist, und die daher nur gleich 1 sein kann. Dadurch ist ε) bewiesen und zugleich das ganze Theorem.

§. 33.

Gruppen vom Grade $p^\alpha q$.

Frobenius hat in der erwähnten Abhandlung den Satz ausgesprochen:

VI. Jede Gruppe vom Grade $p^\alpha q$ ist, wenn p und q von einander verschiedene Primzahlen sind und α einen beliebigen positiven Exponenten bedeutet, metacyklisch.

Der folgende Beweis dieses Satzes entstammt einer brieflichen Mittheilung von Frobenius an den Verfasser.

Zunächst ist klar, dass es genügt, zu beweisen, dass keine Gruppe P vom Grade $p^\alpha q$ einfach ist. Unser Satz ist nämlich bewiesen für $\alpha = 1$. Nehmen wir ihn also für jedes kleinere α schon als bewiesen an, und setzen voraus, dass P einen echten Normaltheiler Q habe, der mehr als das Einheitselement umfasst, so sind die beiden Gruppen Q, P/Q nach der Voraussetzung oder nach dem Satze IV metacyklisch, und also ist auch P metacyklisch.

Wir nehmen also jetzt an, es sei die Gruppe P vom Grade $p^\alpha q$ einfach, und wir haben aus dieser Annahme einen Widerspruch abzuleiten, um ihre Unmöglichkeit nachzuweisen.

α) Zunächst haben wir nach dem Satze I., §. 29 einen Theiler von P vom Grade q. Wir wollen annehmen, es gebe einen

Theiler von P vom Grade $p^\beta q$, wobei $0 \gtreqless \beta < \alpha$ vorausgesetzt ist, und es sei β so gross als möglich angenommen. Dann ist wegen der vorausgesetzten Einfachheit der Gruppe P der Satz §. 28, 2. anwendbar, wonach P isomorph ist mit einer Permutationsgruppe von $p^{\alpha-\beta}$ Ziffern. Unter den Permutationen dieser Gruppe giebt es auch solche, deren Grad durch q theilbar ist, und die also, in ihre Cyklen zerlegt, einen Cyklus von q Ziffern enthalten müssen, und daraus folgt:

(1) $$p^{\alpha-\beta} > q.$$

β) Es sei nun zweitens Q ein Theiler von P vom Grade p^α und Index q. Da nach der Voraussetzung P einfach ist, so kann die in §. 30 mit R bezeichnete Gruppe, die aus den mit Q vertauschbaren Elementen von P besteht, nicht mit P identisch sein, da sonst Q ein Normaltheiler von P wäre, was doch, da P als einfache Gruppe vorausgesetzt ist, unmöglich ist. Da aber Q ein Theiler von R ist, und der Index von Q in Bezug auf P eine Primzahl, so muss $R = Q$ sein. Nach II, §. 30 giebt es also q und nicht mehr von einander verschiedene conjugirte Gruppen

$$Q, Q_1, Q_2, \ldots Q_{q-1},$$

die alle vom Grade p^α sind. Unter diesen Gruppen nehmen wir zwei, etwa Q, Q_1, die einen grössten gemeinschaftlichen Theiler Q_0 vom Grade p^γ haben, und wir nehmen diese beiden Gruppen so gewählt an, dass γ so gross als möglich wird. Es ist dann $0 \gtreqless \gamma < \alpha$. Wenden wir nun auf die Gruppe P das Theorem §. 28, 3. an, indem wir für die beiden Gruppen Q, R jenes Theorems die Gruppe Q setzen, so ist

$$q = h_1 + h_2 + h_3 + \cdots,$$

und darin ist $h_1 = 1$, und die übrigen Summanden $h_2, h_3, \ldots$ sind die Indices von grössten gemeinschaftlichen Theilern von Q mit je einer der Gruppen $Q_1, Q_2, \ldots$ Also sind $h_1, h_2, \ldots$ durch $p^{\alpha-\gamma}$ theilbar, und es folgt

$$q \equiv 1 \pmod{p^{\alpha-\gamma}},$$

also

(2) $$q > p^{\alpha-\gamma},$$

und folglich wegen (1):

(3) $$\gamma > \beta, \quad \gamma > 0.$$

γ) Ist nun also Q_0 der Durchschnitt von Q und Q_1 vom Grade γ, so können wir nach §. 31, III. einen Theiler R von Q vom Grade $p^{\gamma+1}$ bestimmen, von dem Q_0 ein Normaltheiler ist, und R

ist dann in keiner der Gruppen $Q_1, Q_2, \ldots, Q_{q-1}$ enthalten, weil angenommen war, dass Q mit keiner dieser Gruppen einen Theiler gemein hat, dessen Grad grösser als p^γ ist. Ebenso können wir einen Theiler R_1 von Q_1 vom Grade $p^{\gamma+1}$ finden, von dem Q_0 Normaltheiler ist, und der in keiner der Gruppen $Q, Q_2, \ldots, Q_{q-1}$ enthalten ist. Nun ist R sowohl als R_1 in P enthalten. Wir betrachten die kleinste Gruppe S, die R und R_1 zugleich enthält, die jedenfalls in P enthalten ist (das kleinste gemeinschaftliche Vielfache von R und R_1). Der Grad dieser Gruppe S kann nicht eine Potenz von p sein, da sonst nach dem Satze II., §. 30 S und mithin R und R_1 in einer der Gruppen $Q, Q_1, \ldots, Q_{q-1}$ enthalten sein müssten. Es ist aber R nur in Q, R_1 nur in Q_1 enthalten; also ist diese Annahme unzulässig. Der Grad von S muss also von der Form $p^\lambda q$ sein.

Es kann aber λ nicht kleiner als α sein; denn es ist, da eine Gruppe vom Grade $p^{\gamma+1}$ in S enthalten ist, nämlich R,

$$(4) \qquad \lambda \geqq \gamma + 1 > \beta.$$

Nach der in α) gemachten Voraussetzung ist aber in P kein Theiler vom Grade $p^\lambda q$ enthalten, in dem λ zugleich grösser als β und kleiner als α ist. Nach (4) ist also nothwendig $\lambda = \alpha$, d. h. S ist mit P identisch.

Nun ist Q_0 ein Normaltheiler von R und R_1. Fassen wir also alle Elemente c von P, die der Bedingung

$$c^{-1} Q_0 c = Q_0$$

genügen, zu einer Gruppe zusammen, so enthält diese Gruppe sowohl R als R_1, und ist also die ganze Gruppe P. Es ist also Q_0 auch Normaltheiler von P. Da nach (3) γ grösser als Null ist, so ist der Grad von Q_0 grösser als 1, und wir stossen auf einen Widerspruch mit der Annahme, dass P einfach sei.

§. 34.

Einfache Gruppen.

Die Sätze, die wir in den vorhergehenden Paragraphen kennen gelernt haben, gestatten ziemlich weitgehende Schlüsse über die Natur der Gruppen. Sie zeigen, dass wenigstens bei den niedrigeren Gradzahlen die metacyklischen (und cyklischen) Gruppen entschieden überwiegen. Um so höheres Interesse beanspruchen

die wenigen darunter enthaltenen nicht metacyklischen und besonders die einfachen nicht cyklischen Gruppen.

Es ist bis jetzt nicht gelungen, die Gradzahlen der einfachen Gruppen in einem bestimmten Gesetze zusammenzufassen, und man hat sich begnügt, einerseits mit Hülfe der oben entwickelten Sätze, andererseits durch besondere Methoden alle einfachen Gruppen bis zu gewissen Grenzen der Gradzahlen zu ermitteln. Hölder hat diese Untersuchungen für die Gradzahlen bis 200 und Cole für die Gradzahlen bis 500 durchgeführt[1]). Von einfachen nicht cyklischen Gruppen haben sich dabei nur die auch schon aus anderen Untersuchungen bekannten von den Graden 60, 168, 360 ergeben. Es ist ferner noch eine einfache Gruppe vom Grade 660 bekannt, und neuerdings haben Cole und Moore noch auf eine einfache Gruppe vom Grade 504 aufmerksam gemacht[2]). Diese Untersuchungen werden mit dem Wachsen der Gradzahlen sehr mühsam. Wir wollen uns hier auf die Betrachtung der Gradzahlen des ersten Hunderts beschränken.

Hier erweist sich nach den drei allgemeinen Sätzen von Sylow und Frobenius die Mehrzahl der Gruppen als metacyklisch, und es bleiben nur die Gradzahlen

$$36, 60, 72, 84, 90, 100$$

übrig. Dass aber eine Gruppe 36sten Grades nicht einfach sein kann, ergiebt sich nach dem Sylow'schen Satze. Denn eine solche Gruppe müsste einen Theiler 9ten Grades haben und müsste also durch die Permutationen von vier Ziffern darstellbar sein. Das ist aber unmöglich, weil es nur 24 Permutationen von vier Ziffern giebt. Eine Gruppe vom Grade $72 = 8 . 9$ muss nach §. 30, II., da 8 nicht $\equiv 1 \pmod 3$ ist, einen Theiler vom Grade 18 enthalten, und wäre also, wenn sie einfach wäre, ebenfalls durch die Permutationen von vier Ziffern darstellbar, was noch weniger möglich ist. Dass einfache Gruppen von den Graden 84 und 100 nicht existiren können, ergiebt sich gleichfalls sofort aus den Sylow'schen Sätzen, da, wenn wir die Gruppen 7ten oder 25sten Grades aussondern, kein Theiler übrig bleibt, der nach dem Modul 7 oder 5 mit 1 congruent ist. Dass alle diese Gradzahlen nur metacyklischen Gruppen angehören können, folgt dann nach §. 6, 2. ohne Weiteres daraus, dass die Gruppen, deren Grade

[1]) Hölder, Mathematische Annalen, Bd. 40. Cole, American Journal, Vol. 14. — [2]) Bulletin of the New York mathem. society, Oct. 1893.

echte Theiler dieser Zahlen sind, schon als metacyklisch erwiesen sind.

Es bleibt nur noch die Untersuchung der Zahlen 60 und 90 übrig. Dass eine einfache Gruppe vom 60sten Grade existirt, wissen wir schon; nämlich die alternirende Gruppe der Permutationen von fünf Buchstaben (Bd. I, §. 177). Es ist aber noch fraglich, ob dies die einzige ist.

Eine einfache Gruppe P vom Grade 60 enthält nach §. 29, I. als Theiler eine Gruppe 5ten Grades und eine Gruppe 3ten Grades. Nimmt man in dem zweiten Sylow'schen Satze (§. 30) für Q die Gruppe 5ten Grades, so muss R vom 10ten Grade sein, weil der Index von R congruent mit 1 nach dem Modul 5, also nur $= 6$ sein kann. Also kann die Gruppe P vom 60sten Grade nach §. 28, 2. als transitive Permutationsgruppe von sechs Ziffern dargestellt werden; sie kann aber keine cyklische Permutation von nur drei Ziffern enthalten, weil sie als einfache Gruppe (nach Bd. I, §. 158, 2.) primitiv sein muss, und daher, wenn sie einen dreigliedrigen Cyklus enthielte, nach Bd. I, §. 153, 10. die ganze alternirende Gruppe 360sten Grades enthalten müsste. Wir können also eine der Permutationen 3ten Grades in der Form annehmen:

$$a = (1, 2, 3)\,(4, 5, 6).$$

Hierzu wollen wir eine Permutation 5ten Grades, b, fügen, die nur eine cyklische sein kann. Lassen wir darin die Ziffer 6 fehlen, so können wir statt b eine solche Potenz von b nehmen (die ja auch in P vorkommen muss), dass etwa 1, 2 die beiden ersten Ziffern werden, und dann bleiben noch sechs Möglichkeiten für b übrig:

$$(1, 2, 3, 4, 5),\ \ (1, 2, 4, 3, 5),\ \ (1, 2, 4, 5, 3),$$
$$(1, 2, 3, 5, 4),\ \ (1, 2, 5, 3, 4),\ \ (1, 2, 5, 4, 3);$$

von diesen sechs Annahmen sind aber wieder die drei in einer Reihe stehenden nicht wesentlich (d. h. nur durch die Bezeichnung) verschieden. Denn ersetzt man z. B. bei der zweiten Annahme $b = (1, 2, 4, 3, 5)$ das Element a durch a^2 und b durch b^3, so erhält man

$$(1, 3, 2)\,(4, 6, 5);\ \ (1, 3, 2, 5, 4),$$

was durch Vertauschung der Ziffern 2 mit 3 und 4 mit 5 in die erste Annahme übergeht. Die dritte Annahme $b = (1, 2, 4, 5, 3)$ geht, wenn man b durch b^4 und a durch a^2 ersetzt und dann

1 mit 2 und 4 mit 5 vertauscht, in die erste über, und ebenso lassen sich die drei anderen Annahmen über b auf einander zurückführen. Es bleiben also nur zwei Möglichkeiten zu untersuchen:

$$a = (1, 2, 3)(4, 5, 6), \quad b = (1, 2, 3, 4, 5)$$
$$a = (1, 2, 3)(4, 5, 6), \quad b = (1, 2, 3, 5, 4).$$

Davon ist aber die erste zu verwerfen, weil sie in

$$a^2 b = (1, 4, 6)$$

einen dreigliedrigen Cyklus ergeben würde, der nicht vorkommen kann. Es bleibt also nur die einzige Möglichkeit:

$$a = (1, 2, 3)(4, 5, 6), \quad b = (1, 2, 3, 5, 4),$$

und es giebt also, wenn man äquivalente Gruppen als nicht verschieden betrachtet, nur eine einfache Gruppe 60sten Grades.

Diese beiden Elemente a, b kann man als erzeugende Elemente der ganzen Gruppe betrachten und man kann durch ihre wiederholte Zusammensetzung auf sehr mannigfaltige Art die ganze Gruppe vom 60sten Grade herleiten. Wir bekommen ausser dem Einheitselemente die Permutationen 5ten Grades:

$$(2, 3, 6, 5, 4), \quad (1, 3, 5, 6, 4), \quad (1, 2, 5, 4, 6),$$
$$(1, 2, 6, 3, 5), \quad (1, 2, 4, 6, 3), \quad (1, 2, 3, 5, 4),$$

die mit ihren Potenzen 24 ergeben; ferner die Permutationen 3ten Grades:

$$\begin{array}{ll} (1, 2, 3)(4, 5, 6), & (1, 3, 5)(2, 4, 6), \\ (1, 2, 4)(3, 6, 5), & (1, 3, 6)(2, 4, 5), \\ (1, 2, 5)(3, 6, 4), & (1, 4, 5)(2, 3, 6), \\ (1, 2, 6)(3, 4, 5), & (1, 4, 6)(2, 3, 5), \\ (1, 3, 4)(2, 6, 5), & (1, 5, 6)(2, 3, 4), \end{array}$$

die mit ihren Quadraten zusammen 20 ergeben. Endlich erhält man noch 15 Permutationen 2ten Grades:

$$\begin{array}{lll} (1, 2)(3, 4), & (1, 2)(5, 6), & (3, 4)(5, 6), \\ (1, 3)(4, 5), & (1, 3)(2, 6), & (2, 6)(4, 5), \\ (1, 4)(2, 5), & (1, 4)(3, 6), & (2, 5)(3, 6), \\ (1, 5)(2, 3), & (1, 5)(4, 6), & (2, 3)(4, 6), \\ (1, 6)(2, 4), & (1, 6)(3, 5), & (2, 4)(3, 5), \end{array}$$

von denen je drei in einer Reihe stehenden mit dem Einheitselemente zusammen eine Gruppe 4ten Grades bilden.

Dass diese Gruppe auch dargestellt werden kann durch die Permutationen von fünf Ziffern, ergiebt sich nun schon daraus,

dass eine einfache Permutationsgruppe 60sten Grades bei fünf Ziffern wirklich existirt, nämlich die alternirende Gruppe.

Man kann aber auch die Thatsache dadurch verificiren, dass man einen Theiler 12ten Grades von P nachweist (§. 28, 3.). Man erhält diesen Theiler 12ten Grades z. B. daraus, dass die Gruppe 4ten Grades:

$$Q = 1, (1, 2)\,(3, 4),\quad (1, 2)\,(5, 6),\quad (3, 4)\,(5, 6)$$

mit den Permutationen 3ten Grades:

$$c = (1, 3, 5)\,(2, 4, 6)$$

vertauschbar ist, d. h. der Bedingung $c^{-1}Qc = Q$ genügt, und erhält also dann eine Gruppe 12ten Grades:

$$Q,\ Qc,\ Qc^2.$$

Die einfache Gruppe 60sten Grades wird auch die **Ikosaëdergruppe** genannt aus einem Grunde, den wir später kennen lernen werden.

Dieselbe Betrachtung zeigt auch, dass eine einfache Gruppe 90sten Grades nicht existirt. Denn diese Gruppe müsste ein Element 5ten und ein Element 3ten Grades enthalten. Da $90 = 5.18$ ist und 18 keinen anderen Theiler als 6 hat, der nach dem Modul 5 mit 1 congruent ist, so muss, wenn wir für Q eine Gruppe 5ten Grades wählen, R vom Index 6 sein und die Gruppe P wäre also als transitive Permutationsgruppe von sechs Ziffern darstellbar. Ganz wie oben schliesst man, dass sie die beiden Elemente a, b enthalten müsste, was, wie wir gesehen haben, zur Ikosaëdergruppe führt, die nicht Theiler einer Gruppe 90sten Grades sein kann.

§. 35.

Gruppen vom Grade pq.

Es ist nun noch von Interesse, zu untersuchen, wie bei einer gegebenen Gradzahl die Gruppen constituirt sind. Dafür sind die Sätze, die in den vorangegangenen Paragraphen abgeleitet sind, die Grundlagen. Freilich sind wir bis jetzt nur bei den einfacheren Gradzahlen im Stande, die vorhandenen Gruppen vollständig zu übersehen. Am weitesten geht hierin eine Arbeit von Hölder [1]). Wir betrachten hier nur den einfachen Fall,

[1]) Hölder, Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4. Mathematische Annalen, Bd. 43.

dass der Grad pq das Product zweier Primzahlen ist, die auch einander gleich sein können.

Eine solche Gruppe P ist metacyklisch und hat einen Normaltheiler Q vom Grade p, der also eine cyklische Gruppe ist, die wir so darstellen:

(1) $$Q = 1, a, a^2, \ldots a^{p-1} \quad (a^p = 1).$$

Ist nun b ein nicht in Q enthaltenes Element von P, so ist $b^{-1} Q b = Q$.

Wenn b^h die niedrigste Potenz von b ist, die in Q vorkommt, so ist $Q + Qb + \cdots Qb^{h-1}$ eine Gruppe, die mit P identisch sein muss, und folglich muss $h = q$ sein. Wir können also P so darstellen:

(2) $$P = Q + Qb + Qb^2 + \cdots + Qb^{q-1}.$$

Ist nun g eine primitive Wurzel der Primzahl p und ν ein vorläufig noch unbestimmter Exponent, der nach dem Modul $p - 1$ zu nehmen ist, so folgt, da $b^{-1} a b$ in Q enthalten ist,

(3) $$b^{-1} a b = a^{g^\nu},$$

woraus sich für jeden Exponenten α ergiebt:

(4) $$b^{-1} a^\alpha b = a^{\alpha g^\nu},$$

und durch wiederholte Zusammensetzung mit b:

(5) $$b^{-\beta} a^\alpha b^\beta = a^{\alpha g^{\nu \beta}}.$$

Nun ist jedenfalls $b^{pq} = 1$, und wenn wir also in (5) $\beta = pq$ setzen, so folgt, dass für jedes α

$$a^{\alpha g^{\nu pq}} = a^\alpha,$$

also $g^{\nu pq} \equiv 1 \pmod p$ oder

(6) $$\nu p q \equiv 0 \pmod{p - 1}$$

sein muss. Hieraus schliesst man weiter, dass, wenn $p - 1$ nicht durch q theilbar ist, was immer eintritt, wenn $p = q$ ist, ν durch $p - 1$ theilbar, also nach (3)

$$a b = b a,$$

und in Folge dessen auch für jedes $\alpha, \beta, \alpha', \beta'$:

$$a^\alpha b^\beta = b^\beta a^\alpha, \quad a^\alpha b^\beta a^{\alpha'} b^{\beta'} = a^{\alpha'} b^{\beta'} a^\alpha b^\beta,$$

d. h. dass die Gruppe eine Abel'sche sein muss. Diesen Fall haben wir aber schon im zweiten Abschnitte dieses Bandes untersucht und gefunden, dass es, wenn $p = q$ ist, zwei Gruppen (mit

den beiden Invarianten p, p oder mit einer Invariante p^2), und wenn p von q verschieden ist, eine Gruppe (mit den beiden Invarianten p, q) giebt.

Es bleibt uns also noch der Fall

$$p \equiv 1 \pmod q$$

zu untersuchen, in dem ν jeden der Bedingung

$$\nu \equiv 0 \left(\operatorname{mod} \frac{p-1}{q}\right)$$

genügenden Werth haben kann, deren es q nach dem Modul $p - 1$ verschiedene giebt, nämlich:

$$\nu = 0, \ \frac{p-1}{q}, \ 2\frac{p-1}{q}, \ \ldots \frac{(q-1)(p-1)}{q}. \tag{7}$$

Der Fall $\nu = 0$ führt auch hier auf eine Abel'sche Gruppe. Es sind aber auch die anderen Werthe von ν zulässig, die zu ebenso vielen nicht commutativen Gruppen führen. Diese nicht commutativen Gruppen sind unter einander isomorph und werden auf einander zurückgeführt, wenn man b durch ein b^β ersetzt, wie die Formel (5) zeigt.

Wir können $b^q = 1$ annehmen, denn es ist gewiss b^q in Q enthalten und $b^{pq} = 1$. Wenn also b^q nicht $= 1$ ist, so ersetzen wir b durch b^p.

Man erhält eine der nicht commutativen Gruppen, wenn man in

$$\Theta = a^\alpha b^\beta \tag{8}$$

α die Reihe der Zahlen $0, 1, \ldots p - 1$ und β die Zahlen $0, 1, \ldots q - 1$ durchlaufen lässt. Die Zusammensetzung zweier Elemente dieser Gruppe ergiebt sich nach (5) aus

$$b^\beta a^\alpha = a^{\alpha g^{-\nu\beta}} b^\beta, \quad a^p = 1, \ b^q = 1, \tag{9}$$

wodurch man jedes Compositum aus Elementen Θ auf die Form Θ zurückführen kann.

Um zu zeigen, dass die Elemente (8) nach den Compositionsregeln (9) wirklich eine Gruppe bilden, hat man die Eigenschaften der Gruppe, nämlich, dass aus $\Theta\,\Theta' = \Theta\,\Theta''$ und aus $\Theta'\,\Theta = \Theta''\Theta$ folgt, dass $\Theta' = \Theta''$ ist, und ferner das associative Gesetz

$$\Theta\,(\Theta'\,\Theta'') = (\Theta\,\Theta')\,\Theta''$$

nachzuweisen. Beides aber ergiebt sich sehr leicht aus der Zusammensetzung, die aus (9) folgt:

$$a^\alpha b^\beta a^{\alpha'} b^{\beta'} = a^{\alpha + \alpha' g^{-\nu\beta}} b^{\beta + \beta'}. \tag{10}$$

§. 36.

Grenzen des Index eines Theilers der symmetrischen Permutationsgruppe.

Wir beschliessen diese Betrachtungen mit dem Beweise eines Satzes über Permutationsgruppen, der durch die Schwierigkeit, die sein Beweis anfangs bot, eine gewisse Berühmtheit erlangt hat, und der für die Beurtheilung algebraischer Fragen von Wichtigkeit ist [1]).

Es handelt sich dabei um die symmetrische Permutationsgruppe P von n Ziffern und um ihre Theiler von möglichst kleinem Index. Wir wissen, dass die Gruppe P immer einen Theiler vom Index 2 hat, nämlich die alternirende Gruppe. Ausserdem ist noch ein Theiler vom Index n bekannt, der alle Permutationen von P umfasst, die eine Ziffer ungeändert lassen, der also intransitiv ist.

Zunächst gilt der folgende Satz:

I. Der Index eines imprimitiven Theilers von P ist immer grösser als n, und der Index eines intransitiven Theilers ist gleich oder grösser als n, und nur dann gleich n, wenn der Theiler eine Ziffer in Ruhe lässt, und die übrigen $n - 1$ Ziffern auf alle mögliche Arten permutirt.

Nehmen wir an, es sei Q ein imprimitiver Theiler von P vom Index j, und es bestehen r Systeme der Imprimitivität von je s Ziffern, so dass $n = rs$ ist. Eine Zahl, die der Grad der Gruppe Q sicher nicht übersteigen kann, erhalten wir, wenn wir alle Permutationen in jedem einzelnen der r Systeme und dann noch sämmtliche Permutationen der Systeme abzählen. Der Grad von Q ist also kleiner oder gleich dem Producte $[\Pi(s)]^r \, \Pi(r)$, wenn für jede ganze Zahl n

$$\Pi(n) = 1.2.3 \ldots n$$

---

[1]) Bertrand, Journal de Mathématiques, Tome XV (1845). Serret, Algèbre supér., Section IV, Chapitre III. C. Jordan, Traité des substitutions, p. 67. Netto, Substitutionentheorie, Capitel VI. Crelle's Journ., Bd. 100.

ist, und folglich ist

(1) $$j \gtreqless \frac{\Pi(n)}{[\Pi(s)]^r\, \Pi(r)}.$$

Es ist leicht einzusehen, dass diese Zahl, wenn keiner der Factoren r, s gleich 1 ist, grösser als n ist. Dies ergiebt sich, wenn wir den Quotienten so schreiben:

$$\frac{\Pi(n)}{[\Pi(s)]^r\, \Pi(r)} = \frac{(r+1)(r+2)\ldots n}{(2.3\ldots s)^r} =$$
$$\frac{n}{2}\cdot\left(\frac{r+1}{2}\cdot\frac{r+2}{2}\cdots\frac{2r-1}{2}\right)\left(\frac{2r}{3}\cdot\frac{2r+1}{3}\cdots\frac{3r-1}{3}\right)\cdots$$
$$\left(\frac{(s-1)r}{s}\cdot\frac{(s-1)r+1}{s}\cdots\frac{n-1}{s}\right).$$

Denn hiernach ist

(2) $$j > \frac{n}{2}\left(\frac{r+1}{2}\right)^{r-1}\left(\frac{2r}{3}\right)^r\cdots\left(\frac{(s-1)r}{s}\right)^r.$$

Die Factoren $\frac{r+1}{2}, \frac{2r}{3}, \ldots \frac{(s-1)r}{s}$ sind alle gleich oder grösser als 1, denn es ist

$$\frac{(h-1)r}{h} - 1 = \frac{(h-1)(r-1)-1}{h},$$

also immer positiv, und der erste Factor

$$\left(\frac{r+1}{2}\right)^{r-1}$$

ist grösser als 2, wenn $r > 2$ ist. Ist aber $r = 2$, so ist das Product der beiden Factoren:

$$\left(\frac{r+1}{2}\right)^{r-1}\left(\frac{2r}{3}\right)^r = \frac{3}{2}\left(\frac{4}{3}\right)^2 = \frac{8}{3} > 2,$$

und folglich ist unter allen Umständen $j > n$.

Ist zweitens die Gruppe Q intransitiv, und zerfällt das System der n Ziffern in zwei Systeme von je a und b Ziffern, so dass die Ziffern dieser beiden Systeme durch Q nur unter einander vertauscht werden, und $n = a + b$ ist, so sind alle Permutationen von Q in der Gruppe enthalten, die aus allen Permutationen der a und der b Ziffern besteht; d. h. der Grad von Q ist gleich oder kleiner als $\Pi(a)\,\Pi(b)$, und folglich der Index j von Q

(3) $$j \gtreqless \frac{\Pi(n)}{\Pi(a)\,\Pi(b)} = \frac{n}{1}\,\frac{n-1}{2}\cdots\frac{b+1}{a}.$$

Nehmen wir, was freisteht, an, dass $b \geqq a$ sei, so ist der Ausdruck auf der rechten Seite dieser Ungleichung grösser als n, und nur dann gleich n, wenn $b = n - 1$, $a = 1$ ist. In diesem speciellen Falle kann $j = n$ werden, aber nur dann, wenn die $n - 1$ Elemente durch Q auf alle möglichen Arten permutirt werden, was in dem Satze I. ausgesprochen ist.

Die Ausdrücke (3) für die untere Grenze von j sind nichts Anderes, als die Binomialcoëfficienten $B_a^{(n)}$, deren Bildung sofort zeigt, dass sie bis zur Mitte hin, d. h. so lange $2a \lesseqgtr n$, eine wachsende Zahlenreihe bilden.

Wir wollen für den weiteren Gebrauch hieraus den Schluss ziehen:

α) Ist $a = 1$, lässt also die Gruppe Q eine Ziffer ungeändert, so ist ihr Grad ein Theiler von $\Pi(n-1)$, ist aber $a > 1$, so ist der Grad von Q $\lesseqgtr \Pi(n-2)\, \Pi(2)$.

Der Satz, den wir ferner noch beweisen wollen, lautet nun:

II. Ausser der alternirenden Gruppe giebt es keinen transitiven und primitiven Theiler Q von P, dessen Index $\lesseqgtr n$ ist, ausgenommen in den beiden Fällen $n = 4$, $n = 6$.

Beim Beweise machen wir Gebrauch von den Sätzen (§. 153, 9., 10. des ersten Bandes), dass ein transitiver und primitiver Theiler von P, der nicht die ganze alternirende Gruppe enthält, und daher nicht mit der alternirenden oder der symmetrischen Gruppe selbst identisch ist, keine Transposition und keine cyklische Permutation von nur drei Ziffern enthalten kann.

Es sei also P die symmetrische Permutationsgruppe der n Ziffern $0, 1, 2 \ldots n-1$ und Q ein primitiver und transitiver Theiler von P vom Index j, der nicht die alternirende Gruppe enthält. Es sei ferner P in die Nebengruppen zerlegt:

$$(4) \qquad P = Q + Q\pi_1 + Q\pi_2 + \cdots + Q\pi_{j-1}.$$

Wir betrachten das System der Transpositionen:

$$(5) \qquad (0, 1), (0, 2), \ldots (0, n-1),$$

deren keine in Q vorkommen kann. Ist nun $j < n$, so müssen wenigstens zwei dieser Permutationen, etwa $(0, 1)$, $(0, 2)$, in der-

selben Nebengruppe, etwa in $Q\pi_1$, vorkommen, und folglich giebt es zwei Permutationen $\varkappa_1$, $\varkappa_2$ in Q, die der Bedingung

$$\varkappa_1 \pi_1 = (0, 1), \quad \varkappa_2 \pi_1 = (0, 2)$$

genügen. Es ist daher

$$\varkappa_1 \pi_1 \pi_1^{-1} \varkappa_2^{-1} = \varkappa_1 \varkappa_2^{-1} = (0,1)(0,2) = (0,1,2)$$

in Q enthalten. Dies aber widerspricht unserer Voraussetzung, dass Q keinen dreigliedrigen Cyklus enthalten soll. Demnach kann j nicht $< n$ sein. Ist aber $j = n$, also der Grad von Q gleich $\Pi(n-1)$, so müssen die $n-1$ Permutationen (5) in $n-1$ verschiedenen Nebengruppen vorkommen, und P lässt sich so darstellen:

$$P = Q + Q(0,1) + Q(0,2) + \cdots + Q(0,n-1). \tag{6}$$

Betrachten wir irgend eine andere Transposition, z. B. (2, 3), so kann diese nicht in Q und nicht in $Q(0, 2)$ oder in $Q(0, 3)$ vorkommen, weil sonst $(2, 3)(0, 2) = (0, 2, 3)$ oder $(2, 3)(0, 3) = (0, 3, 2)$ in Q vorkäme. Wir können also, ohne die Allgemeinheit zu beeinträchtigen, annehmen, dass (2, 3) in $Q(0, 1)$ vorkommt, und daraus ergiebt sich:

β) Die Gruppe Q enthält das Transpositionspaar

$$(0, 1)(2, 3). \tag{7}$$

Die Gruppe Q hat einen Theiler Q_0, der aus allen den Permutationen besteht, die die Ziffer 0 an ihrer Stelle lassen. Da Q transitiv ist, so ist, wenn $\varkappa_1, \varkappa_2, \ldots, \varkappa_{n-1}$ Elemente aus Q sind, die 0 in 1, in 2, ..., in $n-1$ überführen,

$$Q = Q_0 + Q_0\varkappa_1 + \cdots + Q_0\varkappa_{n-1}, \tag{8}$$

und da Q vom Grade $\Pi(n-1)$ ist, so folgt hieraus, dass Q_0 vom Grade

$$g = \frac{\Pi(n-1)}{n} \tag{9}$$

ist. Da g eine ganze Zahl, also $\Pi(n-1)$ durch n theilbar sein muss, so schliessen wir zunächst, dass der Fall $j = n$ niemals eintreten kann, wenn n eine Primzahl ist, und für diesen Fall ist also unser Theorem II. bewiesen.

Im Allgemeinen können wir aber schliessen:

γ) Ist n nicht $= 4$, so sind die $n-1$ Ziffern $1, 2, \ldots, n-1$ durch Q_0 noch transitiv verbunden.

Wäre nämlich Q_0 in diesen $n-1$ Ziffern intransitiv, so müsste nach α)

$$\text{entweder } \Pi(n-2) \text{ theilbar durch } g,$$
$$\text{oder } \Pi(n-3)\,\Pi(2) \gtreqless g$$

sein; also nach (9):

$$\text{entweder } \frac{n}{n-1} \text{ eine ganze Zahl, also } n \gtreqless 2(n-1)$$
$$\text{oder } n^2 - 5n + 2 \lesseqgtr 0.$$

Das Eine ist unmöglich, wenn $n > 2$ ist, das Andere, wenn $n > 4$ ist.

Wir sehen von dem Falle $n = 4$ ab und betrachten jetzt den Theiler $Q_{0,1}$ von Q, der die beiden Ziffern 0, 1 ungeändert lässt.

Da $Q_{0,1}$, als Permutationsgruppe der $n-1$ Ziffern betrachtet, ein transitiver Theiler von Q_0 ist, so ist, wie man durch nochmalige Anwendung der Zerlegung (8) schliesst, der Grad g_1 von $Q_{0,1}$ gleich $g : n-1$, also

$$(10) \qquad g_1 = \frac{\Pi(n-1)}{n(n-1)} = \frac{\Pi(n-2)}{n}.$$

Daraus schliessen wir ähnlich wie oben:

δ) Ist n nicht $=6$, so sind die $n-2$ Ziffern $2, 3, \ldots, n-1$ durch $Q_{0,1}$ transitiv verbunden.

Denn wären sie es nicht, so müsste nach α):

$$\text{entweder } \Pi(n-3) \text{ theilbar durch } g_1,$$
$$\text{oder } \Pi(n-4)\,\Pi(2) \gtreqless g_1$$

sein; also nach (10):

$$\text{entweder } \frac{n}{n-2} \text{ eine ganze Zahl, also } n \gtreqless 2n-4,$$
$$\text{oder } n^2 - 7n + 6 \lesseqgtr 0.$$

Das Erste ist nicht möglich, wenn $n > 4$, das Zweite, wenn $n > 6$ ist.

Ist nun $n > 6$, so gilt noch Folgendes:

ε) Die Gruppe $Q_{0,1,2}$, die die drei Ziffern 0, 1, 2 ungeändert lässt, hat den Grad

$$g_2 = \frac{g_1}{n-2} = \frac{\Pi(n-3)}{n},$$

und es ist nicht möglich, dass durch die ganze Gruppe $Q_{0,1,2}$ noch eine vierte Ziffer 3 ungeändert bleibt.

Der Grad g_2 ergiebt sich genau wie der von Q_0 und $Q_{0,1}$. Wenn aber durch $Q_{0,1,2}$ noch eine vierte Ziffer 3 ungeändert bliebe, so wäre g_2 ein Theiler des Grades der symmetrischen Gruppe von $n-4$ Ziffern, also ein Theiler von $\Pi(n-4)$. Es müsste also

$$\frac{n\,\Pi(n-4)}{\Pi(n-3)} = \frac{n}{n-3}$$

eine ganze Zahl sein, also $n \gtreqless 2n-6$ oder $n \lesseqgtr 6$.

Aus ε) schliessen wir, dass es in Q eine Permutation $\varkappa$ giebt, durch die 0, 1, 2, 3 in 0, 1, 2, 4 übergeht, worin 4 eine von 3 verschiedene Ziffer ist. Nach β) enthält also Q auch die Permutation:

$$\varkappa^{-1}(0, 1)(2, 3)\varkappa = (0, 1)(2, 4),$$

folglich auch:

$$(0, 1)(2, 3)(0, 1)(2, 4) = (2, 3, 4),$$

also einen dreigliedrigen Cyklus, was der Voraussetzung widerspricht. Hiernach ist das Theorem II. vollständig bewiesen.

Dass die Fälle $n=4$ und $n=6$ wirklich Ausnahmen bilden, geht aus Bd. I, §. 160 und §. 182 hervor, wo wir gesehen haben, dass die symmetrische Permutationsgruppe von vier Ziffern einen transitiven Theiler vom Index 3 und die von sechs Ziffern einen transitiven Theiler vom Index 6 besitzt.

ZWEITES BUCH.

LINEARE GRUPPEN.

Sechster Abschnitt.

Gruppen linearer Substitutionen.

---

§. 37.

Lineare Substitutionen und ihre Zusammensetzung.

Eines der wirksamsten Mittel zur Bildung von Gruppen, auf welches zugleich viele Anwendungen führen, sind die linearen Substitutionen und ihre Zusammensetzung. Wir sind schon mehrfach solchen linearen Substitutionen begegnet und haben sie z. B. im zweiten Abschnitte des ersten Bandes bei Gelegenheit des Multiplicationsgesetzes der Determinanten, und sodann im elften Abschnitte bei den äquivalenten Zahlen betrachtet.

Unter einer linearen Substitution von n Variablen verstehen wir ein System von Gleichungen, durch das ein System von n Veränderlichen $y_1, y_2, \ldots y_n$ linear durch ein anderes System $x_1, x_2, \ldots x_n$ ausgedrückt wird. Wir unterscheiden nach der Anzahl der Variablen unäre, binäre, ternäre, quaternäre Substitutionen, und wollen im Allgemeinen die Zahl der Variablen die Dimension der Substitution nennen. Wir beschränken uns fürs erste auf homogene Substitutionen, so dass, wenn mit $a_i^{(\varkappa)}$ die Coëfficienten bezeichnet werden, die Substitution durch das Gleichungssystem

$$(1) \qquad y_\varkappa = \sum_{1,n}^{i} a_i^{(\varkappa)} x_i \qquad \varkappa = 1, 2, \ldots n$$

dargestellt ist. Oft kommt es auf die Variablen selbst nicht an, so dass eine solche Substitution durch ihre Coëfficienten $a_i^{(\varkappa)}$ hinlänglich gekennzeichnet ist. Man benutzt zuweilen auch zur Be-

zeichnung einer Substitution einen einfachen Buchstaben, etwa A, und setzt dann

$$(2)\qquad A = \begin{pmatrix} a_1^{(1)}, & a_2^{(1)}, & \dots & a_n^{(1)} \\ a_1^{(2)}, & a_2^{(2)}, & \dots & a_n^{(2)} \\ \cdot & \cdot & \cdot & \cdot \\ a_1^{(n)}, & a_2^{(n)}, & \dots & a_n^{(n)} \end{pmatrix}.$$

Wir werden auch abkürzend $A = (a_i^{(\varkappa)})$ setzen und die Determinante der Substitutionscoëfficienten mit $|A|$ bezeichnen. Diese Determinante wird immer von Null verschieden vorausgesetzt. Das Gleichungssystem (1) stellen wir auch symbolisch so dar:

$$(3)\qquad (y_1, y_2, \dots y_n) = A\,(x_1, x_2, \dots x_n),$$

oder noch kürzer:

$$(4)\qquad (y) = A\,(x).$$

Die Substitution:

$$(5)\qquad y_1 = x_1,\ y_2 = x_2, \dots y_n = x_n$$

oder

$$(6)\qquad J = \begin{pmatrix} 1, & 0, & \dots & 0 \\ 0, & 1, & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & \dots & 1 \end{pmatrix}$$

heisst die identische Substitution. Eine Substitution der Form

$$(7)\qquad y_1 = \mu_1 x_1,\quad y_2 = \mu_2 x_2, \dots, y_n = \mu_n x_n$$

oder

$$(8)\qquad M = \begin{pmatrix} \mu_1, & 0, & \dots & 0 \\ 0, & \mu_2, & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & \dots & \mu_n \end{pmatrix}$$

soll eine multiplicative Substitution oder kurz eine Multiplication und die Elemente $\mu_1, \mu_2, \dots, \mu_n$ die Multiplicatoren genannt werden, ein Ausdruck, der sich durch die Gleichungen (7) rechtfertigt.

Nehmen wir eine zweite lineare Substitution der Dimension n an, durch die ein neues System von Variablen z eingeführt wird:

$$(9)\qquad z_i = \sum_{1,n}^{h} b_h^{(i)} y_h,\quad (z) = B(y),$$

und führen für y die Werthe aus (1) ein, so erhalten wir die z

durch die x ausgedrückt mittelst einer neuen linearen Substitution E, die wir so bezeichnen können:

$$z = E(x) = BA(x), \tag{10}$$

und die Substitution $E = BA$ heisst aus B und A zusammengesetzt oder componirt. Es ist dabei aber zwischen AB und BA zu unterscheiden. Zwei Substitutionen A, B von der besonderen Eigenschaft, dass $AB = BA$ ist, heissen mit einander vertauschbar oder commutativ. Die Substitutionscoëfficienten von E ergeben sich durch Einsetzen der Ausdrücke (1) in (9):

$$z_k = \sum^h e_h^{(k)} x_h,$$

$$e_h^{(k)} = \sum_{1,n}^{i} b_i^{(k)} a_h^{(i)}. \tag{11}$$

Diese Formeln sind ganz dieselben, die wir im §. 27 des ersten Bandes benutzt haben [1]), und wir können demnach das in (11) ausgedrückte Gesetz der Composition der Substitutionen so ausdrücken:

1. Um die aus zwei Substitutionen B, A zusammengesetzte Substitution BA zu bilden, verfährt man ganz so, als ob die beiden Determinanten $|B|$, $|A|$ nach der Multiplicationsregel mit einander multiplicirt werden sollten. Es sind dabei, um die Elemente einer Zeile zu bilden, die Elemente einer Zeile der ersten Componente mit den entsprechenden Elementen der Colonnen der zweiten Componente zu multipliciren und dann zu addiren. Man drückt dies auch kurz so aus, dass in der ersten Componente nach Zeilen, in der zweiten nach Colonnen summirt wird.

Aus dieser Regel ergiebt sich die Folgerung:

2. Die Determinante einer zusammengesetzten Substitution ist gleich dem Producte aus den Determinanten der Componenten.

---

[1]) Nur war dort aus einem leicht ersichtlichen Grunde die Bezeichnung etwas anders.

Um drei Substitutionen derselben Dimension, C, B, A, zusammenzusetzen, muss man die Ausdrücke (10) für z in eine neue lineare Substitution

(12) $$(u) = C(z)$$

einführen und die Variablen u durch die x ausdrücken:

(13) $$(u) = CBA(x).$$

Da es offenbar gleichgültig ist, ob man die Ausdrücke (10) in (12) einführt, oder ob man zuerst z nach (9) durch y und dann y nach (4) durch x ausdrückt, so gilt für diese Composition das associative Gesetz:

(14) $$C(BA) = (CB)A = CBA,$$

was sich auch leicht durch Rechnung bestätigen lässt, wenn man nach (11) die Elemente von $C(BA)$ und $(CB)A$ bildet. Man findet für beide den Ausdruck:

$$\sum^{i} \sum^{h} c_i^{(k)} \, b_h^{(i)} \, a_l^{(h)}.$$

Wir sprechen also den Satz aus:

3. Bei der Zusammensetzung der linearen Substitutionen gilt das associative, aber nicht immer das commutative Gesetz.

Eine Multiplication, bei der alle Multiplicatoren einander gleich sind, also

$$N = \begin{pmatrix} \nu, & 0, & \dots & 0 \\ 0, & \nu, & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & \dots & \nu \end{pmatrix}$$

soll eine Aehnlichkeitssubstitution genannt werden, und zwei Substitutionen, die, wie A und AN oder A und NA, durch Zusammensetzung mit einer Aehnlichkeitssubstitution aus einander abgeleitet werden können, heissen ähnliche Substitutionen. Aus dem Gesetze der Composition ergeben sich sofort die Sätze:

4. Eine Aehnlichkeitssubstitution ist mit jeder Substitution A derselben Dimension vertauschbar; zwei Aehnlichkeitssubstitutionen, mit einander componirt, geben wieder eine Aehnlichkeitssubstitution, und zwei mit einer dritten ähnliche Substitutionen sind auch unter einander ähnlich.

Ebenso leicht erhalten wir:

5. **Durch Zusammensetzung mit der identischen Substitution J wird keine Substitution geändert.**

Die Substitution J wird also bei der Composition als Einheit betrachtet, und kann, wo sie mit anderen Substitutionen componirt auftritt, weggelassen werden.

Nun gilt weiter der Satz:

6. **Zu jeder Substitution A giebt es eine und nur eine inverse Substitution A^{-1}, die der Bedingung**

$$AA^{-1} = A^{-1}A = J \tag{15}$$

genügt.

Dieser letzte Satz ergiebt sich aus den Grundformeln der Determinantentheorie, wenn man die Elemente $\alpha_h^{(k)}$ von A^{-1} aus den linearen Gleichungen

$$\sum^i a_i^{(h)} \alpha_k^{(i)} = 0, \quad h \gtrless k \\ = 1, \quad h = k \tag{16}$$

bestimmt, aus denen sich, wenn wir mit $A_h^{(k)}$ die Unterdeterminanten von $|A|$ bezeichnen,

$$|A|\, \alpha_h^{(k)} = A_k^{(h)} \tag{17}$$

ergiebt, und die das andere System

$$\sum^i \alpha_i^{(h)} a_k^{(i)} = 0, \quad h \gtrless k \\ = 1, \quad h = k \tag{18}$$

zur Folge haben. Die inverse Substitution zu A ist nichts Anderes, als die Auflösung des Gleichungssystems (1) der directen Substitution A, so dass aus $(y) = A(x)$ folgt:

$$(x) = A^{-1}(y). \tag{19}$$

Für die Composition der inversen Substitutionen ergiebt sich aus $ABB^{-1}A^{-1} = J$ der Satz:

$$(AB)^{-1} = B^{-1}A^{-1}. \tag{20}$$

Sind A, B, C drei Substitutionen, so ergiebt sich durch Zusammensetzung mit A^{-1} aus jeder der beiden Gleichungen

$$AB = AC, \quad BA = CA,$$

dass $B = C$ sein muss. Demnach sind für die Zusammensetzung der Substitutionen die charakteristischen Merkmale für eine Gruppe erfüllt, und es ist also der Inbegriff aller Substitutionen

von bestimmter Dimension eine (unendliche) Gruppe (§. 1). Wenn wir aus dieser Gesammtheit irgend eine Menge herausheben, die so in sich abgeschlossen ist, dass irgend zwei ihrer Elemente durch Composition ein Element derselben Menge ergeben, so bildet diese Menge gleichfalls eine Gruppe, die endlich oder unendlich sein kann.

Bedeutet L eine feste Substitution, so kann man aus jeder Substitution A von derselben Dimension eine Substitution

(21) $$A' = L^{-1} A L$$

ableiten, die die Transformirte von A durch L heisst.

Setzen wir

(22) $$(x) = L(x'), \quad (y) = L(y'),$$

so folgt aus (4):

(23) $$(y') = A'(x'),$$

so dass der Uebergang zu der transformirten Substitution gleichbedeutend ist mit der gleichzeitigen Transformation beider Reihen von Veränderlichen durch L^{-1}.

Ist

$$A' = L^{-1} A L, \quad B' = L^{-1} B L,$$

so folgt aus den Gesetzen der Composition:

$$A' B' = L^{-1} A B L,$$

und daraus also der Satz:

7. Durchläuft A die Substitutionen einer Gruppe, so durchläuft bei feststehendem L die Transformirte $L^{-1} A L$ die Substitutionen einer isomorphen Gruppe.

Von den inversen Substitutionen sind wohl zu unterscheiden die transponirten Substitutionen.

Man erhält nämlich aus jeder Substitution A eine bestimmte andere, die die transponirte Substitution zu A heisst, und die wir für den Augenblick mit A_1 bezeichnen wollen, wenn man in A die Zeilen zu Colonnen macht, und umgekehrt, wenn man also in (2) die oberen mit den unteren Indices der a vertauscht.

Wenn man in der Summe (11), $\sum^{i} b_i^{(k)} a_h^{(i)}$, die unteren mit den oberen Indices und gleichzeitig a mit b vertauscht, so erhält man einen Ausdruck, der nach (11) gleich $c_k^{(h)}$ ist.

Diese Bemerkung giebt die Vorschrift, nach der die transponirten Substitutionen zusammengesetzt werden, die sich in dem Satze ausspricht:

8. Sind A_1, B_1 die Transponirten zu A, B, so ist $A_1 B_1$ die Transponirte zu BA. In Zeichen:

$$(BA)_1 = A_1 B_1. \tag{24}$$

Wenn wir die Substitutionsformeln (1) mit einem unbestimmten Factor η_k multipliciren und dann die Summe in Bezug auf k nehmen, so folgt:

$$\Sigma\, y_k \eta_k = \sum^{i} \sum^{k} x_i\, a_i^{(k)} \eta_k, \tag{25}$$

oder wenn wir

$$\sum^{k} a_i^{(k)} \eta_k = \xi_i \tag{26}$$

setzen,

$$\Sigma\, y_k \eta_k = \Sigma\, x_i\, \xi_i. \tag{27}$$

Wenn wir also die Substitutionen (1) durch (4) darstellen, so sind die Formeln (26) der Ausdruck für die Substitution

$$(\xi) = A_1(\eta),$$

und wir können also noch den Satz aussprechen:

9. Sind A, A_1 transponirte Substitutionen von einander von der Dimension n, und sind x, y, ξ, η vier Systeme von Variablen, die mit einander durch die Substitutionen

$$(y) = A(x), \quad (\xi) = A_1(\eta) \tag{28}$$

zusammenhängen, so besteht die Identität

$$y_1 \eta_1 + y_2 \eta_2 + \cdots y_n \eta_n = x_1 \xi_1 + x_2 \xi_2 + \cdots x_n \xi_n. \tag{29}$$

Wenn zwei Reihen von Variablen mit

$$\begin{matrix} x_1, & x_2, & \ldots & x_n \\ \xi_1, & \xi_2, & \ldots & \xi_n \end{matrix}$$

gleichzeitig durch die Substitutionen (28) in zwei neue Reihen

$$\begin{matrix} y_1, & y_2, & \ldots & y_n \\ \eta_1, & \eta_2, & \ldots & \eta_n \end{matrix}$$

transformirt werden, so heissen die beiden Variablenreihen mit einander contragradient, und die Formeln (28) stellen zwei mit einander contragradiente Transformationen dar.

§. 38.

Substitution der Verhältnisse.

Wir haben schon oben gesehen, dass zwei mit einer dritten ähnliche Substitutionen gleicher Dimension unter einander ähnlich sind. Demnach können wir alle mit einander ähnlichen Substitutionen n^{ter} Dimension in eine Classe vereinigen, und jede Substitution kann in einer und nur in einer solchen Classe untergebracht werden. Die einzelnen Substitutionen einer Classe heissen die Repräsentanten der Classe, und jede Classe ist durch irgend einen ihrer Repräsentanten völlig bestimmt.

Ist A ähnlich mit A', B ähnlich mit B', so ist auch AB ähnlich mit $A'B'$.

Bezeichnen wir also mit $\mathfrak{A}$, $\mathfrak{B}$ die Classen, in die A, A' und B, B' gehören, so gelangt man immer in dieselbe Classe, welchen Repräsentanten aus $\mathfrak{A}$ und aus $\mathfrak{B}$ man auch zusammensetzen mag. Diese Classe, die durch AB oder $A'B'$ repräsentirt wird, nennen wir daher aus $\mathfrak{A}$ und $\mathfrak{B}$ zusammengesetzt und bezeichnen sie mit $\mathfrak{A}\mathfrak{B}$. Bei dieser Zusammensetzung gelten dieselben Regeln, wie bei der Zusammensetzung der Substitutionen selbst, und die Gesammtheit der Classen bildet also auch eine Gruppe.

Diese Auffassung der Substitutionen und ihrer Zusammensetzung ist immer dann zweckmässig, wenn es, wie z. B. in der projectiven Geometrie, nur auf die Verhältnisse der Variablen ankommt, und wir bezeichnen daher die Substitutionsclassen als Substitutionen der Verhältnisse.

Wir werden aber diese Substitutionen der Verhältnisse ebenso bezeichnen, wie die anderen Substitutionen, nämlich jede Classe durch einen Repräsentanten, wodurch nicht leicht ein Missverständniss entstehen wird. Den Repräsentanten kann man nach sehr verschiedenen Gesichtspunkten auswählen.

Oft empfiehlt es sich, ihn so anzunehmen, dass die Determinante $= 1$ ist. Dadurch ist aber bei einer Substitution n^{ter} Dimension die multiplicative Substitution (μ) nur bis auf eine n^{te} Einheitswurzel bestimmt. Sind die Repräsentanten so gewählt, so bleibt die Eigenschaft bei der Composition erhalten, und diese Repräsentanten der Classen bilden also auch unter sich eine Substitutionsgruppe.

Im Gebiete der binären Substitutionen ist die Substitution A:

$$(y_1, y_2) = \begin{pmatrix} a, b \\ c, d \end{pmatrix} (x_1, x_2)$$

ls Substitution der Verhältnisse aufgefasst, gleichbedeutend mit er linearen gebrochenen Substitution:

$$\eta = \frac{a\xi + b}{c\xi + d},$$

'enn $\xi = x_1 : x_2$ und $\eta = y_1 : y_2$ gesetzt wird; kommt eine weite Substitution A':

$$(z_1, z_2) = \begin{pmatrix} a', b' \\ c', d' \end{pmatrix} (y_1, y_2),$$

der

$$\zeta = \frac{a'\eta + b'}{c'\eta + d'}$$

inzu, so erhält man die zusammengesetzte Substitution

$$A'' = A'A,$$

urch welche ζ durch ξ ausgedrückt wird:

$$\zeta = \frac{a''\xi + b''}{c''\xi + d''},$$

ach den Regeln der Composition in der Form

$$\begin{pmatrix} a'', b'' \\ c'', d'' \end{pmatrix} = \begin{pmatrix} a', b' \\ c', d' \end{pmatrix} \begin{pmatrix} a, b \\ c, d \end{pmatrix} = \begin{pmatrix} a'a + b'c, & a'b + b'd \\ c'a + d'c, & c'b + d'd \end{pmatrix}.$$

Ist eine solche Substitution multiplicativ, hat sie also die Form

$$\begin{pmatrix} a, 0 \\ 0, d \end{pmatrix},$$

werden wir auch das Verhältniss $a : d$ den Multiplicator ennen.

§. 39.

Permutationen als lineare Substitutionen.

Die Wichtigkeit der linearen Substitutionen und besonders er daraus gebildeten endlichen Gruppen für die Algebra ergiebt sich daraus, dass die Permutationsgruppen von n Elementen als specielle Fälle solcher Substitutionsgruppen aufgefasst erden können.

Bezeichnen wir nämlich mit $x_1, x_2, \ldots, x_n$ ein System von n Veränderlichen, und mit $\alpha_1, \alpha_2, \ldots \alpha_n$ irgend eine Anordnung der n Ziffern 1, 2, ... n, so bestimmen die Gleichungen:

(1) $$x_1 = x'_{\alpha_1}, \quad x_2 = x'_{\alpha_2}, \ldots x_n = x'_{\alpha_n}$$

eine lineare Substitution n^{ter} Dimension:

(2) $$A = \begin{pmatrix} a_1^{(1)}, & \ldots & a_n^{(1)} \\ \cdot & \cdots & \cdot \\ a_1^{(n)}, & \ldots & a_n^{(n)} \end{pmatrix}, \quad (x) = A\,(x'),$$

bei der in jeder Zeile und in jeder Colonne nur ein Coëfficient von Null verschieden ist, und dieser eine den Werth 1 hat.

Die Determinante $|A|$ der Substitution ist also $= \pm 1$. Setzt man aber nach Ausführung der Substitution für x'_i wieder x_i, so ist das Ergebniss nichts Anderes, als die Permutation

$$\begin{pmatrix} 1, & 2, & \ldots & n \\ \alpha_1, & \alpha_2, & \ldots & \alpha_n \end{pmatrix}$$

der Indices von x.

Ist B eine zweite ebenso gebildete Substitution

(3) $$(x') = B\,(x''),$$

oder ausführlicher:

(4) $$x'_1 = x''_{\beta_1}, \quad x'_2 = x''_{\beta_2}, \ldots, x'_n = x''_{\beta_n},$$

so ergiebt die Zusammensetzung nach den Regeln des §. 37:

(5) $$x_1 = x''_{\beta_{\alpha_1}}, \quad x_2 = x''_{\beta_{\alpha_2}}, \ldots x_n = x''_{\beta_{\alpha_n}},$$

was abgekürzt durch

(6) $$(x) = A\,B\,(x'')$$

zu bezeichnen ist.

Nach Bd. I, §. 148 ist aber (nach der Zusammensetzung der Permutationen):

(7) $$\begin{pmatrix} 1, & 2, & \ldots & n \\ \alpha_1, & \alpha_2 & \ldots & \alpha_n \end{pmatrix} \begin{pmatrix} 1, & 2, & \ldots & n \\ \beta_1, & \beta_2 & \ldots & \beta_n \end{pmatrix} = \begin{pmatrix} 1, & 2, & \ldots & n \\ \beta_{\alpha_1}, & \beta_{\alpha_2} & \ldots & \beta_{\alpha_n} \end{pmatrix}.$$

Fassen wir also die Substitutionen A, B als Permutationen der Indices auf, so ist die Substitution $A\,B$ gleichbedeutend mit der zusammengesetzten Permutation $A\,B$.

Die Permutationsgruppen von n Ziffern sind hiernach nichts Anderes, als ein specieller Fall endlicher Gruppen linearer Substitutionen n^{ter} Dimension.

Die Permutationen der ersten Art entsprechen Substitutionen mit der Determinante $+1$, und die Permutationen der zweiten Art Substitutionen mit der Determinante -1.

Dies ergiebt sich einfach daraus, dass eine Transposition, z. B. (1, 2), der Substitution

$$\begin{pmatrix} 0, & 1, & 0, & \ldots & 0 \\ 1, & 0, & 0, & \ldots & 0 \\ 0, & 0, & 1, & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & 0, & \ldots & 1 \end{pmatrix},$$

deren Determinante — 1 ist, entspricht, und dass man alle Permutationen der ersten Art aus einer geraden, und alle Permutationen der zweiten Art aus einer ungeraden Anzahl von Transpositionen zusammensetzen kann.

§. 40.

Die Invarianten von endlichen Gruppen linearer Substitutionen.

Wir beschränken jetzt unsere Betrachtungen auf endliche Gruppen linearer homogener Substitutionen. Das Beispiel der Permutationsgruppen zeigt, dass es solche Gruppen giebt. Andere werden wir später noch kennen lernen.

Wir bezeichnen eine solche Gruppe mit S, und ihre Substitutionen mit $A, B, C, \ldots$ Werden in irgend einer Function der Variablen $x_1, x_2, \ldots, x_n$ die Variablen (x) durch $A(x)$ ersetzt, so sagen wir, die Substitution A werde auf die Variablen (x) angewandt. Wir definiren nun zunächst folgenden Begriff:

1. Eine Form $\Phi(x_1, x_2, \ldots, x_n)$ von n Variablen heisst eine Invariante oder invariante Form der Gruppe S, wenn sie ungeändert bleibt, wenn auf die Variablen (x) die sämmtlichen Substitutionen $A, B, C, \ldots$ der Gruppe S angewandt werden.

Wie früher (Bd. I, §. 15) ist hier unter einer Form eine ganze homogene Function der Variablen x zu verstehen.

Wir können diese Definition auch durch die Formeln:

(1) $$\Phi[A(x)] = \Phi[B(x)] = \Phi[C(x)] \ldots$$

ausdrücken.

Dass es für jede endliche Gruppe S invariante Formen in beliebiger Menge giebt, ist leicht einzusehen. Man braucht nur

eine beliebige Form $\varphi(x)$ der n Veränderlichen x zu nehmen, die Functionen:

(2) $$\varphi[A(x)],\ \varphi[B(x)],\ \varphi[C(x)], \ldots$$

für alle Substitutionen der Gruppe zu bilden, und irgend eine symmetrische Function der Formen (2) für Φ zu nehmen.

Denn wendet man auf (x) eine Substitution der Gruppe S an, so ändert sich die Gesammtheit der Functionen (2) nicht; es wird nur ihre Reihenfolge eine andere.

Man kann den Begriff der Invarianten noch allgemeiner fassen, wie folgt:

2. Eine Form $\Psi(x_1, x_2, \ldots x_n)$ heisst auch dann eine Invariante der Gruppe S, wenn sie constante Factoren annimmt, wenn auf die Variablen (x) die Substitutionen $A, B, C \ldots$ der Gruppe S angewandt werden.

Durch Formeln wird diese Eigenschaft so ausgedrückt:

(3) $$\Psi[A(x)] = \alpha\Psi(x),\ \Psi[B(x)] = \beta\Psi(x),\ \Psi[C(x)] = \gamma\Psi(x) \ldots$$

worin die Coëfficienten $\alpha, \beta, \gamma \ldots$ von den x unabhängig sind.

Wenn eine Unterscheidung nöthig ist, wollen wir die in 1. definirten Formen absolute Invarianten, und die in 2. relative Invarianten der Gruppe S nennen.

Aus den Formeln (3) ergiebt sich:

(4) $$\Psi[AB(x)] = \alpha\beta\,\Psi(x),$$

und daraus folgt, dass die Factoren $\alpha, \beta, \gamma, \ldots$ in ihrer Gesammtheit, bei der Zusammensetzung durch Multiplication, eine Gruppe bilden müssen.

Zwischen dieser (commutativen) Gruppe und der Gruppe S besteht ein im Allgemeinen mehrstufiger Isomorphismus, da verschiedene Substitutionen aus S zu demselben Factor α führen können.

Ist μ der Grad der Gruppe S, so ist der Grad eines jeden Elementes $A, B \ldots$ von S ein Theiler von μ, und folglich ist $A^\mu = B^\mu \cdots$ gleich der identischen Substitution.

Hieraus folgt, dass die Factoren $\alpha, \beta, \gamma \ldots \mu^{\text{te}}$ Einheitswurzeln sind.

Ist e die kleinste positive, der Bedingung

(5) $$\alpha^e = \beta^e = \gamma^e = \cdots = 1$$

genügende Zahl, so sind die $\alpha, \beta, \gamma, \ldots$ zugleich e^{te} Einheits-

wurzeln, und e soll der Index der Invariante $\Psi(x)$ heissen. Ist ε eine primitive e^{te} Einheitswurzel, so können wir

$$\alpha = \varepsilon^a, \quad \beta = \varepsilon^b, \quad \gamma = \varepsilon^c \ldots$$

setzen, und die Exponenten $a, b, c \ldots$ können keinen gemeinschaftlichen Theiler mit e haben. Daraus folgt, dass man die ganzen Zahlen $x, y, z, \ldots$ so bestimmen kann, dass

$$ax + by + cz + \cdots \equiv 1 \pmod e$$

wird (Bd. I, §. 118). Da nun wegen der Gruppennatur unter den Factoren $\alpha, \beta, \gamma, \ldots$ auch die Zahl

$$\alpha^x \beta^y \gamma^z \cdots = \varepsilon$$

vorkommt, so folgt, dass die Gesammtheit der Factoren $\alpha, \beta, \gamma \ldots$ mit den Potenzen von ε:

$$1, \varepsilon, \varepsilon^2, \ldots \varepsilon^{e-1}$$

zusammenfallen muss.

Suchen wir in S alle Substitutionen A, die der Bedingung

$$(4) \qquad \Psi[A(x)] = \Psi(x)$$

genügen, zu denen gewiss die identische Substitution gehört, so erhalten wir eine neue Gruppe T, die ein Theiler von S ist. Bedeutet dann E eine der Bedingung

$$(5) \qquad \Psi[E(x)] = \varepsilon\, \Psi(x)$$

genügende Substitution aus S, so haben alle Substitutionen AE und EA die gleiche Eigenschaft, und wir erhalten die Zerlegung von S in die Nebengruppen:

$$(6) \qquad S = T + TE + TE^2 + \cdots + TE^{e-1};$$

der Index des Theilers T ist also $= \varepsilon$. Zugleich ergiebt sich noch, da jede Substitution $E^{-1}AE$ der Bedingung (4) genügt,

$$(7) \qquad E^{-1}TE = T,$$

woraus hervorgeht, dass T ein Normaltheiler von S ist. Wir haben damit den Satz bewiesen:

3. Ist $\Psi(x)$ eine Invariante der Gruppe S vom Index e, so bilden alle Substitutionen von S, durch die $\Psi(x)$ ungeändert bleibt, einen Normaltheiler T von S vom Index e.

Für die Gruppe T ist $\Psi(x)$ absolute Invariante. Die Invarianten vom Index 1 sind die absoluten Invarianten von S. Die Gruppe T heisst die zur Invariante $\Psi(x)$ gehörige Gruppe.

Hat die Gruppe S vom Grade μ eine Invariante vom Index μ, so wird T die Einheitsgruppe und S ist eine cyklische Gruppe, die aus den Elementen $1, E, E^2 \ldots E^{\mu-1}$ besteht.

Betrachten wir als Beispiel die symmetrische Permutationsgruppe P von n Elementen $x_1, x_2, \ldots, x_n$, die ja nach §. 39 unter den Gruppen linearer Substitutionen enthalten ist, so haben wir als absolute Invarianten die symmetrischen Functionen der n Variablen x. Das Differenzenproduct

$$\sqrt{\Delta} = (x_1 - x_2)(x_1 - x_3) \ldots (x_{n-1} - x_n)$$

ist eine relative Invariante vom Index 2, zu der die alternirende Gruppe gehört. Da die Gruppe P ausser der alternirenden Gruppe keinen Normaltheiler hat und auch nicht cyklisch ist, so giebt es keine relativen Invarianten von höherem Index als 2.

Die absoluten Invarianten, d. h. die symmetrischen Functionen, sind hier durch eine endliche Anzahl solcher Formen rational darstellbar, nämlich durch die symmetrischen Grundfunctionen, und die Invarianten vom Index 2 sind das Product von $\sqrt{\Delta}$ mit absoluten Invarianten. Dass analoge Sätze auch im allgemeinen Falle gelten, werden wir in der Folge beweisen.

Wir schliessen hier mit dem Beweise eines allgemeinen Satzes, der bei allen Anwendungen für die Bildung der Invarianten einer Gruppe S von grossem Nutzen ist.

Im §. 60 des ersten Bandes haben wir für irgend eine Form der n Variablen $F(x_1, x_2, \ldots x_n) = F(x)$ gewisse Formen derselben Variablen $C(x_1, x_2, \ldots x_n) = C(x)$ als Covarianten definirt, die dadurch charakterisirt waren, dass, wenn $F(x)$ durch irgend eine lineare Substitution in eine neue Form $F'(y)$ transformirt wird, die Form C der Bedingung genügt

$$C'(y) = r^{\lambda}\, C(x),$$

wo C' ebenso von den Coëfficienten von F', wie C von den Coëfficienten von F abhängt. Darin bedeutet r die Substitutionsdeterminante, ist also eine Constante. Die Coëfficienten der Form F kommen in C nur homogen vor. Als Beispiel einer Covariante führen wir die Hesse'sche Determinante an.

Wenn nun $F(x)$ eine Invariante der Gruppe S ist, und die y mit den x gleichfalls durch eine Substitution aus S zusammenhängen, so unterscheiden sich die Coëfficienten von F nur durch einen gemeinschaftlichen constanten Factor von den Coëfficienten von F', und Gleiches gilt also auch von den beiden Formen C

und C'. Daraus schliessen wir, dass auch C zu den Invarianten der Gruppe S gehört, und sprechen dies als Satz aus:

4. Bildet man aus einer invarianten Form der Gruppe S beliebige Covarianten, so erhält man neue invariante Formen der Gruppe.

§. 41.

Der Satz von Hilbert.

Der Beweis des Satzes von der Endlichkeit des Invariantensystems einer linearen Substitutionsgruppe beruht auf einem sehr allgemeinen Satze über Formensysteme irgend welcher Art, den Hilbert entdeckt und in mannigfachen Untersuchungen über die Endlichkeit von Invariantensystemen mit ausgezeichnetem Erfolge angewandt hat, zu dessen Ableitung wir jetzt übergehen wollen [1]).

I. Bedeutet $\mathfrak{S}$ irgend ein System von Formen der n Veränderlichen $x_1, x_2, \ldots x_n$ in endlicher oder unendlicher Anzahl, so lässt sich aus $\mathfrak{S}$ eine endliche Anzahl von Formen $F_1, F_2, \ldots, F_\mu$ so auswählen, dass jede Form F von $\mathfrak{S}$ durch einen Ausdruck

$$F = A_1 F_1 + A_2 F_2 + \cdots + A_\mu F_\mu \tag{1}$$

dargestellt werden kann, worin $A_1, A_2, \ldots A_\mu$ Formen der Variablen $x_1, x_2, \ldots x_n$ sind.

Die Definition des Formensystemes $\mathfrak{S}$ muss so vollständig sein, dass von jeder einzelnen Form der Variablen x entschieden ist, ob sie zu $\mathfrak{S}$ gehört oder nicht, ist aber übrigens an keine Voraussetzung gebunden.

Besteht $\mathfrak{S}$ nur aus einer endlichen Zahl von Formen, so ist unser Satz selbstverständlich, denn man kann ja in diesem Falle die sämmtlichen Formen von $\mathfrak{S}$ für $F_1, F_2, \ldots F_\mu$ nehmen. Der Beweis wird sich also nur noch mit dem Falle eines unendlichen Systemes $\mathfrak{S}$ zu befassen haben.

Zur Vereinfachung des Ausdruckes wollen wir das Formensystem $F_1, F_2, \ldots F_\mu$ eine Basis des Systemes $\mathfrak{S}$ nennen. Die Functionen $A_1, A_2, \ldots A_\mu$ müssen so beschaffen sein, dass

---

[1]) Hilbert, „Ueber die Theorie der algebraischen Formen". Mathematische Annalen, Bd. 36 (1890).

die μ Producte $A_1 F_1, A_2 F_2, \ldots, A_\mu F_\mu$ alle von gleichem Grade, dem Grade von F sind. Natürlich aber wird im Allgemeinen nicht gefordert, dass umgekehrt alle Functionen von der Form $A_1 F_1 + A_2 F_2 + \cdots + A_\mu F_\mu$ bei beliebigen A_i zu dem Systeme $\mathfrak{S}$ gehören[1]).

Der Satz, den wir zu beweisen haben, ist evident, wenn es sich um Functionen einer einzigen Veränderlichen x_1 handelt. Denn dann sind alle Formen eines Systemes $\mathfrak{S}$ Potenzen der Variablen x_1 mit nicht negativen Exponenten und mit irgend welchen constanten Coëfficienten multiplicirt. Identisch verschwindende Functionen brauchen wir nicht zu berücksichtigen. Nehmen wir dann für F_1 eine dieser Functionen von möglichst niedrigem Grade, so kann jede andere Function von $\mathfrak{S}$ in der Form eines Productes $A_1 F_1$ dargestellt werden, worin A_1 ebenfalls eine Potenz von x_1 mit nicht negativem Exponenten und constantem Coëfficienten ist.

Um also durch Anwendung der vollständigen Induction zum allgemeinen Beweise zu gelangen, nehmen wir zunächst an, der Satz I. sei als richtig erwiesen für jedes System $\mathfrak{S}_0$ von Formen von n Variablen x und betrachten zunächst ein System $\mathfrak{S}_r$ von Formen F, die ausser den x noch eine $(n+1)^{\text{te}}$ Variable y, aber nicht in höherer als der r^{ten} Potenz enthalten, wenn r irgend eine positive ganze Zahl ist. Jede Function F lässt sich dann auf eine einzige Art in die Form setzen:

$$(2) \qquad F = y^r \varphi + \psi,$$

worin die Variable y in φ gar nicht mehr und in ψ höchstens bis zur $(r-1)^{\text{ten}}$ Potenz vorkommt.

Wenn F das System $\mathfrak{S}_r$ durchläuft, so durchläuft φ ein gewisses System $\mathfrak{S}_0$, das sich nach unserer Voraussetzung durch eine Basis darstellen lässt, nehmen wir an in der Form:

$$(3) \qquad \varphi = a_1 \varphi_1 + a_2 \varphi_2 + \cdots + a_\mu \varphi_\mu.$$

Da nun $\varphi_1, \varphi_2, \ldots, \varphi_\mu$ zu dem Systeme $\mathfrak{S}_0$ gehören, so giebt es Functionen $F_1, F_2, \ldots, F_\mu$ in $\mathfrak{S}_r$, so dass

$$(4) \qquad F_1 = y^r \varphi_1 + \psi_1,\ F_2 = y^r \varphi_2 + \psi_2, \ldots, F_\mu = y^r \varphi_\mu + \psi_\mu,$$

und dass y in $\psi_1, \psi_2, \ldots, \psi_\mu$ höchstens bis zur $(r-1)^{\text{ten}}$ Potenz vorkommt.

---

[1]) Dies findet nur bei besonderen Systemen $\mathfrak{S}$ statt, die man Moduln nennt.

Aus (2), (3), (4) ergiebt sich aber, wenn wir noch

$$\Psi = \psi - a_1 \psi_1 - a_2 \psi_2 \cdots - a_\mu \psi_\mu$$

setzen:

$$(5) \qquad F = a_1 F_1 + a_2 F_2 + \cdots + a_\mu F_\mu + \Psi,$$

worin Ψ die Variable y höchstens bis zum Grade $r-1$ enthält. Alle Functionen Ψ, die der Bedingung (5) genügen, bilden ein System $\mathfrak{S}_{r-1}$.

Wir machen nun weiter die Annahme, das Theorem I. sei bewiesen für Functionen eines jeden Systemes $\mathfrak{S}_{r-1}$. Dann können wir also Ψ durch eine Basis darstellen in der Form:

$$(6) \qquad \Psi = b_1 \Psi_1 + b_2 \Psi_2 + \cdots + b_\nu \Psi_\nu,$$

worin $\Psi_1, \Psi_2, \ldots, \Psi_\nu$ specielle Functionen unseres Systemes $\mathfrak{S}_{r-1}$ sind. Man kann also über die Coëfficienten $a_{i,k}$ so verfügen, dass die Functionen

$$(7) \qquad \begin{aligned} F_1' &= a_{1,1} F_1 + a_{2,1} F_2 + \cdots + a_{\mu,1} F_\mu + \Psi_1 \\ F_2' &= a_{1,2} F_1 + a_{2,2} F_2 + \cdots + a_{\mu,2} F_\mu + \Psi_2 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ F_\nu' &= a_{1,\nu} F_1 + a_{2,\nu} F_2 + \cdots + a_{\mu,\nu} F_\mu + \Psi_\nu \end{aligned}$$

in $\mathfrak{S}_r$ enthalten sind.

Multiplicirt man mit $b_1, b_2, \ldots b_\nu$ und setzt in der Summe nach (5) und (6):

$$\begin{aligned} b_1 \Psi_1 + b_2 \Psi_2 + \cdots + b_\nu \Psi_\nu &= \Psi \\ &= F - a_1 F_1 - a_2 F_2 - \cdots - a_\mu F_\mu, \end{aligned}$$

so folgt

$$(8) \qquad \begin{aligned} F = {} & b_1 F_1' + b_2 F_2' + \cdots + b_\nu F_\nu' \\ & + A_1 F_1 + A_2 F_2 + \cdots + A_\mu F_\mu, \end{aligned}$$

worin

$$(9) \qquad \begin{aligned} A_1 &= a_1 - a_{1,1} b_1 - \cdots - a_{1,\nu} b_\nu \\ &\cdots\cdots\cdots\cdots \\ A_\mu &= a_\mu - a_{\mu,1} b_1 - \cdots - a_{\mu,\nu} b_\nu. \end{aligned}$$

Die Formen $F_1', \ldots F_\nu', F_1, \ldots F_\mu$ gehören dem Systeme $\mathfrak{S}_r$ an und bilden eine Basis dieses Systemes, und das Theorem I. ist also unter der Voraussetzung, dass es für $\mathfrak{S}_0$ gilt, für jedes System $\mathfrak{S}_r$ bewiesen.

Es sei nun $\mathfrak{S}$ ein beliebiges System von Formen von $n+1$ Variablen. Wir greifen irgend eine Form F_0 vom Grade r aus diesem Systeme heraus, und setzen für die Variablen, von denen das System abhängt,

$$(10) \qquad y, \; x_1 + \lambda_1 y, \ldots, x_n + \lambda_n y,$$

worin $\lambda_1, \ldots \lambda_n$ Constanten sind, über die wir so verfügen, dass der Coëfficient von y^r in F_0 nicht verschwindet, d. h. dass $F_0(1, \lambda_1, \ldots \lambda_n)$ von Null verschieden wird. Dann geht das System $\mathfrak{S}$, wie überhaupt jede Form der Variablen (10), in ein System von Formen der Variablen $y, x_1, \ldots x_n$ über, und umgekehrt kann jede Form, die von diesen Variablen abhängt, auch als Form von den linearen Verbindungen (10) dargestellt werden.

Irgend eine Form F des Systemes $\mathfrak{S}$ wird nun nach Potenzen von y geordnet und dann in Bezug auf y die Division mit F_0 ausgeführt, wobei sich

(11) $$F = a_0 F_0 + \Phi$$

ergeben mag, so dass a_0 der Quotient und Φ der Rest der Division ist. a_0 und Φ sind ganze Functionen der Variablen x, y, weil der Coëfficient der höchsten Potenz von y im Divisor F_0 constant ist. Φ übersteigt in Bezug auf y nicht den Grad $r-1$. Durchläuft nun F das System $\mathfrak{S}$, so bildet die Gesammtheit der durch (11) definirten Functionen Φ ein System $\mathfrak{S}_{r-1}$, von dem wir die Darstellbarkeit durch eine Basis als schon erwiesen annehmen. Wir können also setzen:

(12) $$\Phi = A_1 \Phi_1 + \cdots + A_\mu \Phi_\mu,$$

so dass $\Phi_1, \ldots \Phi_\mu$ dem Systeme $\mathfrak{S}_{r-1}$ angehören, d. h. so, dass sich in dem Systeme $\mathfrak{S}$ die Formen

(13) $$F_1 = a_1 F_0 + \Phi_1, \ldots, F_\mu = a_\mu F_0 + \Phi_\mu$$

bestimmen lassen. Setzen wir also

(14) $$A_0 = a_0 - a_1 A_1 - \cdots - a_\mu A_\mu,$$

so folgt aus (11), (12) und (13):

(15) $$F = A_0 F_0 + A_1 F_1 + \cdots + A_\mu F_\mu,$$

wodurch das Theorem I. allgemein bewiesen ist.

§. 42.

Endlichkeit des Invariantensystemes einer endlichen linearen Substitutionsgruppe.

Der im vorigen Paragraphen gegebene Beweis des Satzes I. ist an sich keinerlei Ausnahmen unterworfen. Wir verlieren aber nichts Wesentliches an seiner Allgemeinheit, wenn wir ein- für allemal identisch verschwindende Formen ausschliessen. Wenn

ferner das System $\mathfrak{S}$ Formen 0ten Grades, d. h. von Null verschiedene Constanten enthält, so ist, da wir für F_1 eine solche Constante nehmen können, unser Satz selbstverständlich, da, wenn $A_1 = F : F_1$ gesetzt wird, $F = A_1 F_1$ ist. In dieser Form ist aber der Satz inhaltlos. Wenn wir aber von $\mathfrak{S}$ alle constanten Formen ausschliessen, so bleibt ein System $\mathfrak{S}'$, das keine Formen 0ten Grades mehr enthält, für das unser Satz gleichfalls gilt. Die Basis $F_1, F_2, \ldots F_\mu$ enthält dann gleichfalls keine Formen 0ten Grades, und wir können daher den Satz I. auch so ausdrücken:

II. Alle Formen des Systemes $\mathfrak{S}$ von positivem Grade lassen sich durch eine Basis $F_1, F_2, \ldots F_\mu$, deren Elemente von positivem Grade sind, in der Form ausdrücken:

$$F = \Phi_1 F_1 + \Phi_2 F_2 + \cdots + \Phi_\mu F_\mu. \tag{1}$$

Die Grade von $\Phi_1, \Phi_2, \ldots \Phi_\mu$ sind dann niedriger als der Grad von F.

Die wichtigsten Anwendungen findet dieses Theorem bei Untersuchungen über die Möglichkeit, alle Formen eines gewissen Systemes $\mathfrak{S}$ als ganze rationale Functionen einer endlichen Anzahl unter ihnen darzustellen. Man nennt ein solches Formensystem ein endliches (nicht in dem Sinne, dass es nur aus einer endlichen Zahl von Formen besteht). Es gilt der folgende Satz:

III. Wenn sich die Coëfficienten $\Phi_1, \Phi_2, \ldots \Phi_\mu$ in der Darstellung (1) des Theorems II. für jede Form F in $\mathfrak{S}$ so wählen lassen, dass sie, wenn sie nicht constant sind, selbst dem Systeme $\mathfrak{S}$ angehören, so ist das System $\mathfrak{S}$ endlich.

Dies ergiebt sich unmittelbar daraus, dass die Grade der Formen $\Phi_1, \Phi_2, \ldots \Phi_\mu$ niedriger sind, als der Grad von F. Wendet man also die Darstellung (1) auf die nicht constanten unter den Functionen Φ an, so gelangt man zu Coëfficienten von noch niedrigerem Grade und muss also schliesslich bei wiederholter Anwendung dieses Verfahrens auf Constanten kommen.

Daraus folgt nun durch eine sehr einfache Schlussweise, die ich einer mündlichen Mittheilung von Hurwitz verdanke, die Endlichkeit des Invariantensystemes $\mathfrak{J}$ einer endlichen Gruppe linearer Substitutionen S.

Es sei $F_1, F_2, \ldots, F_\mu$ eine nach II. bestimmte Basis des Systemes $\mathfrak{J}$, und F irgend eine andere nicht constante Invariante von S. Dann lassen sich die Formen $A_1, A_2, \ldots, A_\mu$ so bebestimmen, dass

(2) $$F = A_1 F_1 + A_2 F_2 + \cdots + A_\mu F_\mu$$

wird. Wendet man auf diese identische Gleichung sämmtliche Substitutionen der Gruppe S an, so bleiben nach Voraussetzung $F, F_1, F_2, \ldots F_\mu$ ungeändert, während $A_\varkappa$ in $A_\varkappa, A'_\varkappa, A''_\varkappa \ldots$ übergehen mag. Bildet man die Summe der so aus (2) abgeleiteten Gleichungen und setzt, wenn m den Grad der Gruppe S bedeutet,

(3) $$m\,\Phi_\varkappa = A_\varkappa + A'_\varkappa + A''_\varkappa + \cdots,$$

so folgt:

(4) $$F = \Phi_1 F_1 + \Phi_2 F_2 + \cdots \Phi_\mu F_\mu.$$

Die Functionen $\Phi_1, \Phi_2, \ldots \Phi_\mu$ sind aber nach §. 40 Invarianten von S, und damit ist nach III. die Endlichkeit des Systemes $\mathfrak{J}$ bewiesen.

Derselbe Schluss lässt sich auch auf die relativen Invarianten anwenden, wie folgt:

Wir bezeichnen mit $F(x)$ das ganze System der Functionen, die den Bedingungen §. 40, (3):

$$F[A(x)] = \alpha F(x), \quad F[B(x)] = \beta F(x) \ldots$$

bei feststehenden Factoren $\alpha, \beta, \ldots$, die, wie wir gesehen haben, Einheitswurzeln sind, genügen.

Nach dem Hilbert'schen Satze lässt sich ein specielles System solcher Functionen $F_1, F_2, \ldots, F_m$ derart auswählen, dass man

(5) $$F = A_1 F_1 + A_2 F_2 + \cdots + A_m F_m$$

setzen kann, worin $A_1, A_2, \ldots, A_m$ Formen der Variablen (x) sind. Behandelt man diese Formel so wie die Formel (2), indem man die Substitutionen der Gruppe S darauf anwendet und dann die Summe bildet, so erhält man, entsprechend der Formel (4):

$$F = \Phi_1 F_1 + \Phi_2 F_2 + \cdots + \Phi_m F_m,$$

worin die Coëfficienten $\Phi_1, \Phi_2, \ldots, \Phi_m$ absolute Invarianten sind.

Zur Vervollständigung ist noch hinzuzufügen, dass inhomogene Functionen der Variablen nur dann Invarianten sein können, wenn ihre einzelnen homogenen Bestandtheile Invarianten sind.

Endlich können wir auch noch nach gebrochenen Invarianten fragen. Ist

$$\frac{F(x)}{F_1(x)}$$

eine solche gebrochene Invariante, so nehmen wir zunächst an, die beiden ganzen rationalen Functionen $F(x)$, $F_1(x)$ von den n Variablen x seien von gemeinschaftlichen Theilern befreit (Bd. I, §. 51).

Beschränken wir uns fürs Erste auf absolute Invarianten, und ist demnach

$$\frac{F(x)}{F_1(x)} = \frac{F[A(x)]}{F_1[A(x)]},$$

so haben, da die x hier als unabhängige Variable angesehen werden, weder rechts noch links Zähler und Nenner einen gemeinschaftlichen Theiler, und es folgt:

$$F[A(x)] = \alpha F(x), \quad F_1[A(x)] = \alpha F_1(x),$$

worin α ein constanter Factor ist, der, wie wir früher gesehen haben, eine Einheitswurzel ist. Zähler und Nenner einer gebrochenen Invariante müssen daher selbst, wenn auch nur relative, Invarianten sein.

Wenn wir aber nicht gerade die einfachste Darstellung suchen, so können wir absolute gebrochene Invarianten auch als Quotienten von absoluten ganzen Invarianten darstellen. Wir brauchen den Bruch nur durch eine geeignete Potenz des Nenners zu erweitern, also wenn die α e^{te} Einheitswurzeln sind,

$$\frac{F(x)}{F_1(x)} = \frac{F(x)\,F_1(x)^{e-1}}{[F_1(x)]^e}$$

zu setzen. Hiernach können wir auch alle relativen Invarianten mit einem bestimmten Factorensysteme $\alpha, \beta, \ldots$ darstellen als Product von einer von ihnen mit absoluten Invarianten, die aber gebrochen sein können.

§. 43.

Das Formenproblem.

Im vorigen Paragraphen ist nachgewiesen, dass es zu einer endlichen Gruppe linearer Substitutionen eine endliche Anzahl unabhängiger Invarianten giebt. Ist n die Dimension der linearen

Substitution, so sind diese Formen homogene Functionen von n Variablen, und es können also nicht mehr als n von einander unabhängige existiren. Damit ist nicht gesagt, dass sich alle diese Formen rational durch n unter ihnen ausdrücken lassen, aber zwischen $n+1$ Invarianten muss immer eine rationale Gleichung bestehen, die sich durch Elimination der n Variablen ergiebt.

Es ist aber noch die umgekehrte Frage zu untersuchen, ob es wirklich für eine lineare Substitutionsgruppe von der Dimension n immer n unabhängige Invarianten giebt.

Wenn wir für die Variablen feste Werthe setzen, so erhalten dadurch die sämmtlichen Invarianten der Gruppe gleichfalls bestimmte Werthe. Die Frage, die wir noch zu beantworten haben, ist nun die, ob zu einem Werthsysteme der Invarianten bestimmte Werthsysteme der Variablen, und zwar in endlicher Anzahl, existiren. Wenn dies bewiesen ist, so können wir die Variablen als (mehrwerthige) algebraische Functionen der Invarianten auffassen, und die Anzahl der von einander unabhängigen Invarianten kann nicht kleiner sein, als die Anzahl der Variablen, weil sonst ein Theil der Variablen, wenn die Werthe der Invarianten gegeben sind, noch willkürlich bleiben würde.

Wenn (x) ein einem bestimmten Werthsysteme der Invarianten entsprechendes Werthsystem der Variablen ist, und A eine Substitution der Gruppe S, so entspricht nach der Natur der Invarianten das System $A(x)$ demselben Werthsysteme der Invarianten, und unser Problem hat also mindestens so viele Lösungen, als der Grad der Gruppe beträgt. Dass dies aber die genaue Anzahl der Lösungen ist, geht aus den folgenden Betrachtungen hervor.

In besonderen Fällen, d. h. für besondere Werthe der Invarianten, können von diesen Werthsystemen der Variablen mehrere zusammenfallen. Dies kann aber nur für solche Werthsysteme der (x) geschehen, für die eine Relation von der Form $(x) = A(x)$ besteht, denn aus $A(x) = B(x)$ würde $(x) = A^{-1}B(x)$ folgen, was in der Form $(x) = A(x)$ enthalten ist.

Wir nehmen eine lineare homogene Function Θ der Variablen $x_1, x_2, \ldots x_n$ an, die wir so bezeichnen:

$$(1) \qquad \Theta = \Theta(x) = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n.$$

Bedeutet A eine Substitution der endlichen Gruppe S, so können wir aus $\Theta(x)$ eine neue Function:

(2) $$\Theta[A(x)] = c_1' x_1 + c_2' x_2 + \cdots + c_n x_n$$

ableiten, deren Coëfficienten c_i' nach §. 37, 9. mit den ursprünglichen Coëfficienten c_i durch die zu A transponirte Substitution

$$(c') = A_1(c)$$

zusammenhängen.

Wenn nun $A, B, C, \ldots$ die sämmtlichen Substitutionen der Gruppe S sind, so kann man in gleicher Weise die Functionen

(3) $$\Theta[A(x)],\ \Theta[B(x)],\ \Theta[C(x)], \ldots$$

bilden, die wir auch kürzer durch

(4) $$\Theta, \Theta_1, \Theta_2, \ldots, \Theta_{\mu-1}$$

bezeichnen, wenn μ der Grad der Gruppe S ist.

Nun kann man über die Coëfficienten c_i, die bis jetzt noch ganz willkürlich sind, so verfügen, dass keine zwei der Functionen (4) mit einander identisch werden (Bd. I, §. 143, 1.). Aus (3) aber ergiebt sich:

1. Wenn man in den μ Functionen (4) gleichzeitig irgend eine Substitution aus S anwendet, so ändert sich die Gesammtheit dieser Functionen nicht, sondern sie erleiden nur eine Permutation.

Daraus ergiebt sich ferner:

2. Jede symmetrische Function der Grössen (4) ist eine absolute Invariante der Gruppe S.

Wir bemerken noch, dass man an Stelle der Function Θ irgend eine andere auch nicht lineare, selbst eine gebrochene oder inhomogene Function setzen könnte, wenn nur die μ Functionen (4) von einander verschieden sind.

Bilden wir nun das Product:

(5) $$\Phi(t) = (t-\Theta)(t-\Theta_1)\ldots(t-\Theta_{\mu-1}) \\ = t^\mu + A_1 t^{\mu-1} + A_2 t^{\mu-2} + \cdots + A_\mu,$$

welches eine ganze rationale Function μ^{ten} Grades von t ist, so sind die Coëfficienten $A_1, A_2, \ldots, A_\mu$ nach 2. Invarianten der Gruppe S, und die Grössen $\Theta, \Theta_1, \ldots, \Theta_{\mu-1}$ sind die Wurzeln der Gleichung

(6) $$\Phi(t) = 0.$$

Wir betrachten nun als Rationalitätsbereich Ω den Körper, der aus den absoluten Invarianten der Gruppe S und allen Zahlen[1]) besteht. Diesem Rationalitätsbereich gehören die Coëfficienten von $\Phi(t)$ an, und wir beweisen zunächst den Satz:

3. Die Function $\Phi(t)$ ist in Ω irreducibel.

Ist nämlich $\Psi(t)$ irgend eine Function in Ω, die für $t = \Theta$ verschwindet, so können wir in der Gleichung $\Psi(\Theta) = 0$, da die $x_1, x_2, \ldots, x_n$ unabhängige Variable sind, das System (x) dieser Variablen durch $A(x)$ ersetzen, wenn A irgend eine Substitution aus S ist. Dadurch kann Θ in jede der Functionen $\Theta_1, \Theta_2, \ldots, \Theta_{\mu-1}$ übergeführt werden, während die Coëfficienten von Ψ ungeändert bleiben, und folglich ist $\Psi(\Theta_1) = 0$, $\Psi(\Theta_2) = 0, \ldots \Psi(\Theta_{\mu-1}) = 0$. Es muss also $\Psi(t)$ durch $\Phi(t)$ theilbar sein, wodurch die Irreducibilität erwiesen ist.

Es bedeute nun ω irgend eine Function der Variablen x und

$$\omega, \omega_1, \omega_2, \ldots, \omega_{\mu-1}$$

mögen die Functionen sein, die aus ω durch Anwendung der Substitutionen von S entstehen, von denen nun nicht vorausgesetzt zu werden braucht, dass sie alle von einander verschieden sind. Ist t eine Variable, so ist

$$\Phi(t)\left(\frac{\omega}{t-\Theta} + \frac{\omega_1}{t-\Theta_1} + \cdots + \frac{\omega_{\mu-1}}{t-\Theta_{\mu-1}}\right) = \Psi(t) \tag{7}$$

eine ganze rationale Function $(\mu-1)^{\text{ten}}$ Grades von t, und zugleich ist es eine Invariante von S, also eine Function in Ω. Setzen wir darin $t = \Theta$, so folgt durch einen schon früher oft angewandten Schluss (Bd. I, §. 143, 155):

$$\omega = \frac{\Psi(\Theta)}{\Phi'(\Theta)}, \tag{8}$$

worin der Satz enthalten ist:

4. Jede rationale Function der Variablen (x) kann rational durch Θ ausgedrückt werden, gehört also dem Körper $\Omega(\Theta)$ an.

Aus diesem Satze können wir einen zweiten Beweis dafür ableiten, dass alle Invarianten der Gruppe S rational durch eine endliche Anzahl von ihnen, nämlich die Coëfficienten der Function $\Phi(t)$, darstellbar sind. Denn wenn wir eine absolute In-

[1]) Man kann sich auch auf einen besonderen Zahlkörper beschränken, wenn nur darin die Substitutionscoëfficienten der Gruppe S enthalten sind.

variante J nach dem Satze 4. als rationale Function von Θ darstellen, so kann sich diese nicht ändern, wenn eine der Substitutionen (Θ, Θ_1), (Θ, Θ_2), ... ausgeführt wird, und diese Function ist also rational durch die Coëfficienten von $\Phi(t)$ ausdrückbar. Ob diese Darstellung freilich durch ganze Functionen möglich ist, würde bei diesem Beweise unentschieden bleiben.

Unter den Functionen ω der Variablen x sind auch die Variablen x selbst enthalten, und die Frage, von der wir ausgegangen sind, ob die Variablen x als algebraische Functionen der Invarianten angesehen werden können, ist damit bejahend entschieden.

Die Aufgabe, die Variablen x als algebraische Functionen der Invarianten der Gruppe S darzustellen, also die Bestimmung des Körpers $\Omega(\Theta)$ heisst nach F. Klein das Formenproblem der Gruppe S[1]. Ist die Anzahl der Variablen n, so nennen wir das Formenproblem von der n^{ten} Dimension.

Der Körper $\Omega(\Theta)$ ist ein durch die Gruppe S völlig bestimmter algebraischer Körper über Ω. Er ist ein Normalkörper, denn nach 4. sind die conjugirten Grössen $\Theta, \Theta_1, \Theta_2, \ldots \Theta_{\mu-1}$ alle im Körper $\Omega(\Theta)$ selbst enthalten. Die Gleichung $\Phi(t) = 0$ ist eine Normalgleichung und ist die Galois'sche Resolvente des Formenproblems (Bd. I, §. 145).

5. Die Galois'sche Gruppe des Formenproblems, d. h. die Galois'sche Gruppe der Gleichung $\Phi(t) = 0$, ist mit der Gruppe S isomorph.

Um dies nachzuweisen, bezeichnen wir mit A, B zwei Substitutionen aus S und mit $AB = C$ die daraus zusammengesetzte Substitution. Ist nun

$$\Theta_1 = \Theta[A(x)], \quad \Theta_2 = \Theta[B(x)], \quad \Theta_3 = \Theta[C(x)],$$

so ist die Substitution

$$(\Theta, \Theta_2) = (\Theta_1, \Theta_3),$$

und folglich

$$(\Theta, \Theta_1)(\Theta, \Theta_2) = (\Theta, \Theta_1)(\Theta_1, \Theta_3) = (\Theta, \Theta_3),$$

d. h. die Gruppe der Substitutionen (Θ, Θ_1), (Θ, Θ_2), ... ist mit der Gruppe der A, B, ... isomorph.

Nehmen wir statt der Function Θ eine Function η, die nicht lauter verschiedene Werthe hat, sondern die Substitutionen eines

[1] Vorlesungen über das Ikosaëder, S. 123. (Leipzig 1884.)

Theilers S' von S vom Index j, aber keine anderen gestattet, so genügt η einer Gleichung j^{ten} Grades, die als eine Resolvente des Formenproblems zu betrachten ist. Jede Function, die die Permutationen von S' gleichfalls gestattet, ist dann eine rationale Function von η und von den Invarianten der Gruppe S. Die Resolvente der η ist eine Partial- oder Totalresolvente, je nachdem die Gruppe S' mit den zu ihr conjugirten Theilern von S einen gemeinschaftlichen Theiler hat oder relativ prim ist (Bd. I, §. 156).

§. 44.

Klein's Erweiterung des algebraischen Grundproblems.

Die Betrachtungen, die im vorigen Paragraphen durchgeführt sind, bilden eine directe Verallgemeinerung der Galois'schen Theorie für eine allgemeine Gleichung n^{ten} Grades; und diese Theorie ist als Specialfall in der Theorie der linearen Substitutionsgruppen enthalten.

Es sind nämlich nach §. 39 die symmetrischen Functionen von n unabhängigen Variablen $x_1, x_2, \ldots x_n$ die Invarianten der Gruppe S, die aus den Permutationen dieser n Variablen besteht, und die Gleichung $\Phi(t) = 0$ ist also für diesen Fall nach Bd. I, §. 145 die Galois'sche Resolvente der Gleichung n^{ten} Grades, deren Wurzeln die Grössen x_i sind. Wir können also die allgemeine Aufgabe der Algebra, eine Gleichung n^{ten} Grades aufzulösen, als ein Formenproblem einer linearen Substitutionsgruppe n^{ter} Dimension auffassen. Nun giebt es aber specielle Gleichungen, die durch Formenprobleme von niedrigerer Dimension gelöst werden können, so insbesondere die reinen Gleichungen die durch ein Formenproblem der ersten Dimension lösbar sind.

Lineare homogene Substitutionen von einer Dimension sind nämlich nur von der Form

$$(1) \qquad x' = \alpha x,$$

und wenn diese eine endliche Gruppe vom Grade μ bilden sollen, so müssen die Coëfficienten α Einheitswurzeln vom Grade μ sein. Lassen wir umgekehrt α in (1) sämmtliche μ^{te} Einheitswurzeln durchlaufen, so haben wir eine Gruppe vom Grade μ. Diese Gruppe hat eine absolute Invariante x^μ, und wenn diese gegeben ist, so erhält man x als μ^{te} Wurzel daraus.

Die Auflösung der allgemeinen Gleichungen 2ten, 3ten und 4ten Grades sind also auf Formenprobleme von nur einer Dimension zurückführbar. Wir werden in einem späteren Abschnitte sehen, dass die allgemeine Gleichung 5ten Grades auf ein binäres Formenproblem zurückführbar ist, und man kann sich nun als eine unmittelbare Erweiterung der Aufgabe, die Lösung einer Gleichung auf reine Gleichungen zurückzuführen, die Frage stellen: welches ist die geringste Dimensionenzahl eines Formenproblems, durch das sich eine gegebene Gleichung lösen lässt? Die Aufgabe würde dann so formulirt werden müssen:

Es sollen aus den Wurzeln einer gegebenen Gleichung rationale Functionen in möglichst kleiner Zahl so gebildet werden, dass sie in homogene lineare Functionen ihrer selbst übergehen, wenn die Wurzeln den Permutationen der Galois'schen Gruppe der gegebenen Gleichung unterworfen werden.

Auf diese Weise hat F. Klein die Aufgabe der algebraischen Auflösung einer Gleichung erweitert. Er hat, um die Beantwortung der Frage anzubahnen, für die allgemeine Gleichung 6ten und 7ten Grades bewiesen, dass sie auf quaternäre Formenprobleme zurückgeführt werden können.

Die allgemeine Gleichung n^{ten} Grades ist, wie wir gesehen haben, unmittelbar einem Formenproblem von n Dimensionen äquivalent. Die Frage aber, ob die allgemeine Gleichung n^{ten} Grades, wenn n grösser als 7 ist, einem Formenprobleme von weniger als n Dimensionen entspricht, ist noch nicht beantwortet; sie muss wahrscheinlich verneint werden [1]).

§. 45.

Einfluss relativer Invarianten.

Bei der Definition des Formenproblems im §. 43 haben wir nur die absoluten Invarianten der Gruppe S benutzt. Nun giebt es, wie wir gesehen haben, auch Fälle, in denen ausser den ab-

[1]) F. Klein, Zur Theorie der allgemeinen Gleichungen 6ten und 7ten Grades; Mathematische Annalen, Bd. XXVIII, S. 18. Vergl. auch „The Evanston Colloquium, Lectures on Mathematics by Felix Klein", Lecture IX, London und New York, Macmillan and Co. (1894).

soluten auch relative Invarianten existiren, und diese können zur Vereinfachung des Formenproblems benutzt werden.

Ist r eine solche relative Invariante, so wird eine gewisse Potenz von r, deren Grad e ein Theiler des Grades μ von S ist, eine absolute Invariante, und r wird also durch eine **reine Gleichung** in Ω bestimmt.

Alle Substitutionen von S, durch die r ungeändert bleibt, bilden für sich eine Gruppe T_r, und die Gruppe T_r ist, wie wir in §. 40 gesehen haben, ein Normaltheiler von S.

Ferner aber sehen wir, dass jede Function der Variablen x, die durch die Substitutionen der Gruppe T_r ungeändert bleibt, rational durch r ausgedrückt werden kann, d. h. in dem durch Adjunction von r aus Ω abgeleiteten Körper Ω_r enthalten ist.

Nach §. 40 nämlich giebt es eine Substitution E in S, und eine primitive e^{te} Einheitswurzel ε, so dass r durch E in εr übergeht, und alle Werthe, die r annehmen kann:

$$r,\ \varepsilon r,\ \varepsilon^2 r, \ldots \varepsilon^{e-1} r,$$

erhält man durch Wiederholung der Substitution E. Bedeutet ferner τ eine Function der x, die die Substitutionen der Gruppe T_r gestattet, und durch E und seine Potenzen in

$$\tau,\ \tau_1,\ \tau_2, \ldots \tau_{e-1}$$

übergeht, so gestatten alle diese Functionen gleichfalls die Substitutionen von T_r, weil T_r ein Normaltheiler von S ist. Die Function

(1) $$(\varepsilon^{-h}, \tau) = \tau + \varepsilon^{-h}\tau_1 + \cdots + \varepsilon^{-h(e-1)}\tau_{e-1},$$
$$(h = 0, 1, 2, \ldots e-1),$$

die nach Analogie der Lagrange'schen Resolventen (Bd. I, §. 164) gebildet ist, nimmt durch Anwendung der Substitution E den Factor ε^h an, und wenn wir also

(2) $$(\varepsilon^{-h}, \tau) = r^h \Psi_h$$

setzen, so ist Ψ_h eine absolute Invariante, also im Körper Ω enthalten.

Aus (1) und (2) ergiebt sich aber

(3) $$e\tau = \Psi + r\Psi_1 + r^2\Psi_2 + \cdots + r^{e-1}\Psi_{e-1},$$

wodurch die Behauptung erwiesen ist.

Setzen wir

(4) $$\mu = e\nu,$$

so ist ν der Grad der Gruppe T_r, und wenn die Function Θ, die wir in §. 43 zur Lösung des Formenproblems angewandt haben, durch die Substitutionen von T_r in

$$\Theta, \Theta_1, \ldots \Theta_{\nu-1}$$

übergeht, so ist

$$\Phi_r(t) = (t - \Theta)(t - \Theta_1) \ldots (t - \Theta_{\nu-1})$$

eine Function von t in dem erweiterten Rationalitätsbereiche Ω_r; der Körper $\Omega(\Theta)$ ist identisch mit $\Omega_r(\Theta)$. Er ist also ein algebraischer Körper μ^{ten} Grades über Ω und ν^{ten} Grades über Ω_r. Das Formenproblem μ^{ten} Grades wird demnach durch Adjunction eines Radicals auf ein Formenproblem ν^{ten} Grades zurückgeführt.

§. 46.

Der erweiterte Invariantenbegriff.

Die relativen Invarianten sind im Grunde ein specieller Fall eines allgemeineren Begriffes, den wir in ähnlicher Weise, wie die relativen Invarianten, zur Reduction des Formenproblems anwenden können.

Wir suchen nach Systemen von homogenen Formen gleichen Grades der Variablen $x_1, x_2 \ldots x_n$:

(1) $$X_1, X_2, \ldots X_m,$$

von der Beschaffenheit, dass durch die Anwendungen der Substitutionen der Gruppe S die Functionen $X_1, X_2, \ldots X_m$ ein System Σ von linearen Substitutionen erleiden; die Substitutionen Σ bilden dann gleichfalls eine Gruppe, und zwar eine Gruppe, die mit S ein- oder mehrstufig isomorph ist. Ist $m = 1$, so erhalten wir, wie man sieht, den Begriff der relativen Invarianten. Wir suchen nun alle Substitutionen von S, die jede einzelne der Functionen (1) ungeändert lassen. Diese Substitutionen bilden eine Gruppe, die wir mit T bezeichnen, und von der wir nachweisen wollen, dass sie ein Normaltheiler von S ist. Bezeichnen wir mit s eine Substitution aus S, durch die die X die Substitution σ erleiden, so erleiden die X durch s^{-1} die Substitution σ^{-1}. Ist dann ferner τ eine Substitution aus T, so bleiben durch τ die X ungeändert. Demnach erleiden durch $s^{-1} \tau s$ die X die Substitution $\sigma^{-1} \sigma = 1$, d. h. sie bleiben un-

geändert. $s^{-1}\tau s$ ist also auch in T enthalten, und T ist folglich ein Normaltheiler von S.

Wir bezeichnen mit μ, ν die Grade von S und T und setzen

$$\mu = e\nu;$$

dann ist e der Index von T und zugleich der Grad der Gruppe Σ.

Jede absolute Invariante der Gruppe T, d. h. jede Function von x, die die Substitutionen von T gestattet, kann rational in Ω durch die X ausgedrückt werden.

Dies folgt durch das schon oft angewandte Schlussverfahren: wenn wir mit ϱ eine Function der X bezeichnen, die e verschiedene Werthe $\varrho, \varrho_1, \ldots \varrho_{e-1}$ annimmt, und

$$(2) \qquad \Phi(t) = (t-\varrho)(t-\varrho_1)\ldots(t-\varrho_{e-1})$$

setzen, so ist $\Phi(t)$ eine rationale Function der Variablen t in Ω.

Eine absolute Invariante r von T nimmt höchstens e verschiedene Werthe an, die den Werthen $\varrho, \varrho_1, \ldots \varrho_{e-1}$ entsprechen, nämlich $r, r_1, \ldots r_{e-1}$, wobei unter Umständen auch gleiche Werthe vorkommen können. Die Function von t:

$$\frac{\Phi(t)\, r}{t-\varrho} + \frac{\Phi(t)\, r_1}{t-\varrho} + \cdots + \frac{\Phi(t)\, r_{e-1}}{t-\varrho_{e-1}} = \Psi(t)$$

ist dann in Ω enthalten, und für $t = \varrho$ ergiebt sich:

$$(3) \qquad r = \frac{\Psi(\varrho)}{\Phi'(\varrho)},$$

wodurch, da $\Phi'(\varrho)$ von Null verschieden ist, r rational durch ϱ ausgedrückt ist. Es ist also r im Körper $\Omega\,(X_1, X_2, \ldots X_m)$ enthalten.

Die Invarianten der Gruppe T sind zugleich Invarianten der Gruppe S; durch die Lösung des Formenproblems für die Gruppe Σ sind dann die $X_1, \ldots X_m$ bekannt, also auch die Invarianten der Gruppe T, und das Formenproblem der Gruppe S ist also zurückgeführt auf die successive Lösung der beiden Formenprobleme der Gruppen Σ und T, die von niedrigerem Grade als das Formenproblem für S sind. Ein Formenproblem, was in dieser Weise in zwei Formenprobleme niedrigeren Grades zerlegbar ist, können wir ein imprimitives Formenproblem nennen. Da es für eine solche Reduction nöthig ist, dass T ein von S und von der Einheit verschiedener Normaltheiler von S sei, so ist, wenn S eine einfache Gruppe ist, das entsprechende Formenproblem stets primitiv.

Wir können aber auch umgekehrt schliessen, dass, wenn S einen Normaltheiler vom Index e besitzt, das Formenproblem imprimitiv ist. Wir brauchen nämlich nur, um ein System der Functionen $X_1, \dots X_m$ zu erhalten, eine Invariante ϱ der Gruppe T zu nehmen, die e verschiedene Werthe in S enthält, und können für $X_1, \dots X_m$ geradezu die Werthe $\varrho, \varrho_1, \dots \varrho_{e-1}$ nehmen. Die Gruppe Σ ist dann die durch S unter den ϱ hervorgerufene Permutationsgruppe.

Im Sinne des §. 44 wird es aber immer darauf ankommen, m so klein als möglich zu machen, und eine Reduction des Problems in diesem Sinne wird nur dann erzielt sein, wenn $m < n$ ist.

§. 47.

Normalformen.

Noch eine allgemeine Betrachtung müssen wir anstellen, ehe wir zu speciellen Anwendungen übergehen. Wir haben schon in §. 37 gesehen, dass wir aus jeder Gruppe S von linearen Substitutionen unendlich viele isomorphe Gruppen ableiten können, indem wir mit einer willkürlichen Substitution L von derselben Dimension transformiren, also die transformirte Gruppe

(1) $$L^{-1} S L$$

bilden; und dies ist gleichbedeutend mit der Einführung anderer Variablen y an Stelle von x durch die Substitution

(2) $$(x) = L\,(y).$$

Diese Transformation können wir dazu verwenden, um die Gruppe S in einer einfachen Normalform darzustellen, und dann erhalten auch die Invarianten gewisse feste Normalformen, die in manchen Fällen sehr einfache Gestalten annehmen können. Bilden wir für die Normalform die Resolvente des Formenproblems [§. 43, (8)], die wir jetzt in der Form schreiben wollen:

(3) $$\Phi\,(\Theta, A_1, A_2, \dots) = 0,$$

worin $A_1, A_2, \dots$ Invarianten der Gruppe S bedeuten, so wird auch diese, wenn wir die Normalform benutzen, eine einfache Gestalt erhalten. Die Variablen x_i lassen sich, wie wir gesehen

haben, rational durch Θ und die A_k ausdrücken, und wir setzen

(4) $$x_i = \varphi_i(\Theta, A_1, A_2, \ldots).$$

Auch diese Ausdrücke werden, wenn über die Function Θ verfügt ist, für die Normalform feste Gestalten annehmen.

Nun kann aber auch der Fall vorkommen, dass die Invarianten nicht in der Normalform, sondern in einer beliebigen anderen Form, die wir die allgemeine Form nennen wollen, gegeben sind. Dann wird es sich darum handeln, die Substitution L zu finden, durch die die allgemeine Form in eine von vornherein als möglich erkannte Normalform transformirt wird. Diese Aufgabe ist, wie wir nun sehen wollen, keine andere, als das für die Normalform gestellte Formenproblem selbst.

Nehmen wir an, die Invarianten in der allgemeinen Form, als Functionen von y, seien $B_1, B_2, \ldots$, so dass durch die Substitution (2) die Identitäten

(5) $$A_1 = B_1, \; A_2 = B_2, \ldots$$

hergestellt werden. Es ist die Aufgabe, wenn die Functionen A_i, B_i der Form nach gegeben sind, die Substitution L zu bestimmen, die die Gleichungen (5) zu identischen macht. Diese Aufgabe ist gelöst, wenn wir die Gleichung (3) für ein passend gewähltes specielles Werthsystem der A_i als gelöst voraussetzen. Um dies nachzuweisen, bilden wir die vollständigen Differentiale der Gleichungen (3) und (4):

$$0 = \Phi'(\Theta) d\Theta + \sum^{s} \Phi'(A_s) dA_s$$

$$dx_i = \varphi_i'(\Theta) d\Theta + \sum^{s} \varphi_i'(A_s) dA_s,$$

worin $\Phi'(\Theta)$, $\Phi'(A_s)$, $\varphi_i'(\Theta)$, $\varphi_i'(A_s)$ die partiellen Ableitungen bedeuten. Eliminiren wir $d\Theta$, so folgt:

(6) $$dx_i = \sum^{s} \frac{\varphi_i'(A_s)\,\Phi'(\Theta) - \Phi'(A_s)\,\varphi_i'(\Theta)}{\Phi'(\Theta)}\, dA_s.$$

Nun ist in Folge der Gleichungen (5):

(7) $$dA_s = \sum^{k} B_s'(y_k)\, dy_k,$$

und wenn wir also

(8) $$x_i = \alpha_{1,i} y_1 + \cdots + \alpha_{n,i} y_n$$

(9) $$dx_i = \alpha_{1,i} dy_1 + \cdots + \alpha_{n,i} dy_n$$

setzen, so ergiebt die Vergleichung von (6) mit (9):

$$(10) \qquad \alpha_{k,i} = \sum^{s} \frac{\varphi'_i(A_s)\,\Phi'(\Theta) - \Phi'(A_s)\,\varphi'_i(\Theta)}{\Phi'(\Theta)} B'_s(y_k).$$

Die rechte Seite dieser Gleichungen muss sich also auf eine Constante reduciren, und wir können ihren Werth finden, wenn wir für die y irgend ein specielles Werthsystem setzen, das nur an die eine Bedingung gebunden ist, dass $\Phi'(\Theta)$ nicht verschwindet. Für dieses specielle Werthsystem sind die Werthe der A_i durch die Gleichungen (5) bestimmt, und Θ ist bekannt, wenn wir für dies specielle Werthsystem der A_i das Formenproblem (3) als gelöst voraussetzen. Dann sind durch (10) die Coëfficienten $\alpha_{k,i}$ und damit die Substitution L vollständig bestimmt.

Siebenter Abschnitt.

Gruppen binärer linearer Substitutionen.

---

§. 48.

Ternäre orthogonale Substitutionen.

Es ist nun unsere Aufgabe, aus der Gesammtheit der linearen Substitutionen engere Gruppen auszusondern und schliesslich zu endlichen Gruppen zu gelangen. Solche engere Gruppen, die immer noch unendlich sein können, erhält man, wenn man die Forderung stellt, dass gegebene homogene Functionen der Variablen invariant bleiben sollen. Wir wollen aber die Aufgabe nicht in dieser Allgemeinheit weiter verfolgen, sondern gleich zur Betrachtung des wichtigsten speciellen Falles übergehen. Wir wollen uns auf ternäre Substitutionen beschränken und fordern, dass eine quadratische Form von nicht verschwindender Determinante invariant bleiben soll. Da, wie wir früher gesehen haben (Bd. I, §. 57), jede solche quadratische Form durch lineare Transformation in eine Summe von Quadraten verwandelt werden kann, so beschränken wir das Problem nicht weiter, wenn wir für diese quadratische Form die Summe der Quadrate annehmen. Solche Substitutionen heissen orthogonal.

Die Substitution

(1) $$(y_1, y_2, y_3) = A\,(x_1, x_2, x_3)$$

ist also orthogonal, wenn die Substitutionscoëfficienten so bestimmt sind, dass die Identität besteht:

(2) $$y_1^2 + y_2^2 + y_3^2 = x_1^2 + x_2^2 + x_3^2.$$

Wenn man die Ausdrücke (1) in (2) substituirt und die Coëfficienten entsprechender Glieder einander gleich setzt, so

erhält man sechs Relationen zwischen den neun Coëfficienten von A.

Diese Relationen lauten, wenn

$$(3) \qquad A = \begin{pmatrix} a_1, & a_2, & a_3 \\ b_1, & b_2, & b_3 \\ c_1, & c_2, & c_3 \end{pmatrix}$$

angenommen wird:

$$(4) \qquad \begin{array}{ll} a_1^2 + b_1^2 + c_1^2 = 1, & a_2 a_3 + b_2 b_3 + c_2 c_3 = 0 \\ a_2^2 + b_2^2 + c_2^2 = 1, & a_3 a_1 + b_3 b_1 + c_3 c_1 = 0 \\ a_3^2 + b_3^2 + c_3^2 = 1, & a_1 a_2 + b_1 b_2 + c_1 c_2 = 0, \end{array}$$

und sind aus der analytischen Geometrie wohl bekannt. Für das Quadrat der Substitutionsdeterminante $|A|$ ergiebt sich aus diesen Relationen nach der Multiplicationsregel der Determinanten der Werth 1, und folglich hat $|A|$ den Werth ± 1.

Aus den Formeln (4) ergiebt sich, dass die inverse Substitution zu A

$$A^{-1} = \begin{pmatrix} a_1, & b_1, & c_1 \\ a_2, & b_2, & c_2 \\ a_3, & b_3, & c_3 \end{pmatrix}$$

mit der transponirten identisch ist, und diese Eigenschaft könnte auch als Definition der orthogonalen Substitutionen dienen.

Die Gesammtheit der orthogonalen Substitutionen bildet eine Gruppe. Darunter ist eine engere Gruppe enthalten, die durch den Werth

$$(5) \qquad |A| = +1$$

ausgezeichnet ist, die wir als die Gruppe der eigentlichen orthogonalen Substitutionen bezeichnen wollen.

Man kann die lineare Substitution (1) als den Uebergang von einem rechtwinkeligen Coordinatensysteme zu einem zweiten mit demselben Anfangspunkte deuten, wenn man x_1, x_2, x_3 und y_1, y_2, y_3 als rechtwinkelige Coordinaten eines und desselben (veränderlichen) Punktes in dem ersten und dem zweiten Coordinatensysteme ansieht. Durch A ist die gegenseitige Lage der beiden Coordinatensysteme bestimmt und umgekehrt. Besteht die Bedingung (5), wie wir jetzt voraussetzen wollen, so kann das erste Coordinatensystem mit dem zweiten zur Deckung gebracht werden durch Drehung um eine feste Axe mit einem bestimmten Drehungswinkel.

Denn setzen wir

$$D = \begin{vmatrix} a_1 - 1, a_2, a_3 \\ b_1, b_2 - 1, b_3 \\ c_1, c_2, c_3 - 1 \end{vmatrix},$$

so erhalten wir aus den Relationen (4):

$$|A|\, D = - D,$$

also, wenn (5) besteht, $D = 0$. Demnach lassen sich drei Grössen λ, μ, ν aus den Gleichungen:

$$(6) \qquad \begin{aligned} \lambda &= a_1 \lambda + a_2 \mu + a_3 \nu \\ \mu &= b_1 \lambda + b_2 \mu + b_3 \nu \\ \nu &= c_1 \lambda + c_2 \mu + c_3 \nu \\ \lambda^2 &+ \mu^2 + \nu^2 = 1 \end{aligned}$$

bestimmen, und diese drei Grössen λ, μ, ν bestimmen die Richtung einer geraden Linie, die mit den Axen y_1, y_2, y_3 dieselben Winkel einschliesst, wie mit den Axen x_1, x_2, x_3. Eine in dieser Richtung durch den Coordinatenanfangspunkt gelegte Linie ist die Drehungsaxe.

In dem Falle $|A| = -1$ trifft dieser Schluss nicht mehr zu.

Daneben besteht noch eine andere Deutung der orthogonalen Substitution $(y) = A(x)$, wonach (x) und (y) die Coordinaten zweier verschiedener Punkte x und y sind, bezogen auf ein und dasselbe Coordinatensystem. Wenn x einen Raumtheil (Linie, Fläche oder Körper) überstreicht, so erfüllt der entsprechende Punkt y einen congruenten Raumtheil (wenn $|A| = -1$ ist, einen spiegelbildlich gleichen). Dies wird durch die folgende Betrachtung dargethan.

Die Gruppe der eigentlichen orthogonalen Substitutionen ist äquivalent mit einer Gruppe, die man aus den verschiedenen Stellungen eines um einen festen Punkt drehbaren Körpers bilden kann. Diese Gruppe erhält man, wenn man eine beliebige Stellung E als Einheit annimmt, aus der man in irgend eine andere Stellung A gelangt durch Drehung um eine bestimmte Axe mit einem bestimmten Winkel. Ist B eine dritte Stellung, so hat man unter der zusammengesetzten Stellung AB die Stellung zu verstehen, die man erhält, wenn man die Drehung, die zu A geführt hat, nicht von der Einheitsstellung, sondern von der Stellung B aus vollführt. Denn nimmt man ein mit dem Körper in starrer Verbindung stehendes Axensystem an, z. B. das System der Hauptträgheitsaxen, und bezeichnet mit (x) die Coordinaten

eines beliebigen, im Raume festen Punktes, bezogen auf dies Axensystem in der Einheitsstellung E, so erhält man die Coordinaten desselben Punktes, bezogen auf das Axensystem in der Stellung A oder B durch zwei orthogonale Substitutionen $A(x)$ und $B(x)$.

Demnach sind $AB(x)$ die auf das System A bezogenen Coordinaten eines Punktes y mit den Coordinaten $(y) = B(x)$ im Systeme E. Der Punkt y hat also im Systeme E dieselben Coordinaten, wie der Punkt x im Systeme B, d. h. y liegt zur Einheitsstellung so wie x zur Stellung B. Führen wir nun die Drehung, die von E zu B führt, so aus, dass wir den Punkt x festhalten, aber den Punkt y und das Axensystem A die Drehung begleiten lassen, so gelangt der Punkt y nach x, und die Coordinaten von x, bezogen auf die neue Lage des Systemes A, sind dieselben, wie die des Punktes y in Bezug auf die ursprüngliche Lage von A, d. h. $AB(x)$. Diese neue Lage des Systemes A kann man aber offenbar auch so erreichen, dass man die Drehung, die zu der Stellung A führt, nicht von der Einheitsstellung, sondern von der Stellung B aus vollzieht.

Aus der Gruppe der eigentlichen erhält man die Gesammtheit aller orthogonalen Substitutionen durch Zusammensetzung mit einer uneigentlichen, etwa mit $(x_1, x_2, x_3) = (y_1, y_2, -y_3)$, die, nach der zweiten geometrischen Auffassung, eine Spiegelung an der Ebene x_1, x_2 ist, bei der der Punkt y das Spiegelbild des Punktes x ist.

Von besonderem Interesse sind nun die in der Gesammtheit der eigentlichen orthogonalen Substitutionen enthaltenen endlichen Gruppen, auf die wir später noch näher eingehen werden. Wir wollen hier nur noch über die geometrische Seite dieser Frage Folgendes bemerken. Einer solchen endlichen Gruppe G vom Grade g von orthogonalen Substitutionen entspricht eine endliche Gruppe von Stellungen eines Körpers. Denkt man sich den Körper in diesen verschiedenen Stellungen gleichzeitig fixirt und das Ganze zu einem neuen starren Körper vereinigt, so erhält man ein Gebilde, das in einer endlichen Anzahl g verschiedener Stellungen sich selbst decken kann. Man kann für jede Gruppe Körper von unendlich vielen verschiedenen Gestalten finden. Die anschaulichsten und bekanntesten Verhältnisse ergeben sich, wenn man den Körper von ebenen Flächen begrenzt annimmt.

Solche Gebilde sind die regulären Pyramiden, die Doppelpyramiden und die regulären Körper (Tetraëder, Octaëder, Würfel, Dodekaëder und Ikosaëder).

Die reguläre Pyramide von g Seiten gelangt durch Drehung um die Hauptaxe mit einem Winkel $2\pi : g$ und durch Wiederholung dieser Drehung auf g verschiedene Arten mit sich zur Deckung.

Ist g gerade, so kann man eine reguläre Doppelpyramide von g Seitenflächen ausser durch Drehung um ihre Hauptaxe mit dem Winkel $4\pi : g$ noch (auf $\frac{1}{2}g$ verschiedene Arten) durch Drehung um eine in der Aequatorialebene liegende Axe mit einem Drehungswinkel von 180 Grad mit sich zur Deckung bringen.

Das Tetraëder gestattet 12 verschiedene Stellungen, in denen es denselben Raum einnimmt.

Um sie zu erhalten, bezeichne man den Ort einer Ecke in der Einheitsstellung mit 1. Dann erhält man drei Stellungen des Tetraëders, bei denen die Ecke 1 fest bleibt. Man kann aber jede Ecke an die Stelle von 1 bringen, wodurch die Zahl sich vervierfacht.

Dieselbe Zahl findet man auch, wenn man die Ebene einer Seitenfläche festhält, wobei man noch drei Stellungen des Tetraëders findet, und jede Seitenfläche in die Ausgangsebene bringt.

Endlich kann man auch so zählen, dass man jede Kante auf zwei Arten mit einer festen Strecke zur Deckung bringt. Ebenso verfährt man bei den übrigen regulären Körpern. Man findet so den Grad der Gruppe

gleich dem Producte aus der Anzahl der Ecken mit der Anzahl der in einer Ecke zusammenstossenden Kanten oder Seitenflächen, oder

gleich dem Producte aus der Anzahl der Seitenflächen mit der Anzahl der Seiten oder Ecken einer Grenzfläche, oder

gleich der doppelten Anzahl der Kanten.

Jede dieser Zählungen ergiebt

für das Tetraëder 12 Stellungen,
für das Octaëder und den Würfel 24 Stellungen,
für das Dodekaëder und Ikosaëder 60 Stellungen.

Es sei schliesslich noch bemerkt, dass, anstatt der Stellungen des Körpers, auch die Drehungen selbst als Elemente der Gruppe aufgefasst werden können.

§. 49.

Lineare gebrochene Substitutionen.

Die Gruppe der orthogonalen ternären Substitutionen ist, wie jetzt nachgewiesen werden soll, isomorph mit der Gruppe der linearen gebrochenen Substitutionen einer Veränderlichen, oder der binären Substitutionen der Verhältnisse (§. 38).

Wir bezeichnen eine ternäre orthogonale Substitution mit

(1) $$(y_1, y_2, y_3) = A(x_1, x_2, x_3),$$

(2) $$y_1^2 + y_2^2 + y_3^2 = x_1^2 + x_2^2 + x_3^2.$$

Hierauf wenden wir zunächst nach §. 37, (21) die Transformation durch die feste (nicht orthogonale) Substitution

(3) $$L = \begin{Bmatrix} i, & 0, & 0 \\ 0, & \frac{1}{\sqrt{2}}, & \frac{1}{\sqrt{2}} \\ 0, & \frac{i}{\sqrt{2}}, & \frac{-i}{\sqrt{2}} \end{Bmatrix}, \quad L^{-1} = \begin{Bmatrix} -i, & 0, & 0 \\ 0, & \frac{1}{\sqrt{2}}, & \frac{-i}{\sqrt{2}} \\ 0, & \frac{1}{\sqrt{2}}, & \frac{i}{\sqrt{2}} \end{Bmatrix}$$

an, worin $i = \sqrt{-1}$ ist, deren Determinante den Werth 1 hat, und setzen

(4) $$\begin{aligned} (y_1, y_2, y_3) &= L(y_1', y_2', y_3') \\ (x_1, x_2, x_3) &= L(x_1', x_2', x_3') \end{aligned},$$

(5) $$(y_1', y_2', y_3') = A'(x_1', x_2', x_3'),$$

worin

(6) $$A' = L^{-1} A L$$

gleichfalls eine lineare Substitution bedeutet, deren Determinante $|A'| = |A|$, also gleich ± 1 ist. Die Relation (2) geht durch die Substitutionen (4) in

(7) $$-y_1'^2 + 2y_2' y_3' = -x_1'^2 + 2x_2' x_3'$$

über, woraus sich sechs Relationen zwischen den Coëfficienten von A' ergeben, die wir aber hier nicht aufstellen wollen, da wir die Substitution A' auf andere Weise einfacher finden können.

Wenn wir nämlich unter ξ_1, ξ_2 neue Variable verstehen und

(8) $$x_1' = \sqrt{2}\, \xi_1 \xi_2, \quad x_2' = \xi_1^2, \quad x_3' = \xi_2^2$$

setzen, so verschwindet $x_1'^2 - 2\, x_2' x_3'$ identisch und y_1', y_2', y_3' gehen durch (5) und (8) in binäre quadratische Formen der Variablen ξ_1, ξ_2 über, die nach (7) der Gleichung

(9) $$y_1'^2 - 2\, y_2' y_3' = 0$$

identisch genügen müssen, d. h. $y_2' y_3'$ muss ein vollständiges Quadrat werden. Die quadratischen Formen y_1', y_2', y_3' zerlegen wir nun in je zwei lineare Factoren. Dabei können y_2' und y_3' keinen gemeinsamen Factor haben, da sonst auch der andere Factor in beiden Functionen übereinstimmen und also die drei Coëfficienten von y_2' und y_3' mit einander proportional sein müssten. Dann würde aber $|A'|$ verschwinden, was nicht möglich ist. Demnach ergiebt sich aus (9), dass y_2' und y_3' Quadrate linearer Functionen sein müssen. Setzen wir

(10) $$\eta_1 = \alpha \xi_1 + \beta \xi_2, \quad \eta_2 = \gamma \xi_1 + \delta \xi_2,$$

so können wir also hiernach mit Rücksicht auf (9)

(11) $$y_1' = \sqrt{2}\, \eta_1 \eta_2, \quad y_2' = \eta_1^2, \quad y_3' = \eta_2^2$$

setzen; wenn wir die Multiplicationen ausführen und dann die Substitution (8) im umgekehrten Sinne ausführen, so erhalten wir aus (10) und (11):

$$\begin{aligned} y_1' &= (\alpha\delta + \beta\gamma)\, x_1' + \sqrt{2}\, \alpha\gamma\, x_2' + \sqrt{2}\, \beta\delta\, x_3', \\ y_2' &= \sqrt{2}\, \alpha\beta\, x_1' + \alpha^2 x_2' + \beta^2 x_3', \\ y_3' &= \sqrt{2}\, \gamma\delta\, x_1' + \gamma^2 x_2' + \delta^2 x_3'. \end{aligned}$$

Also lautet die Substitution A':

(12) $$A' = \begin{pmatrix} \alpha\delta + \beta\gamma, & \sqrt{2}\, \alpha\gamma, & \sqrt{2}\, \beta\delta \\ \sqrt{2}\, \alpha\beta, & \alpha^2, & \beta^2 \\ \sqrt{2}\, \gamma\delta, & \gamma^2, & \delta^2 \end{pmatrix}.$$

Durch diese Substitution ist die Bedingung (7) noch nicht völlig befriedigt, sondern es folgt nur, dass die rechte und linke Seite sich durch einen constanten Factor unterscheiden, der von den Coëfficienten $\alpha, \beta, \gamma, \delta$ abhängt. Nun ist aber der Coëfficient von $x_1'^2$ in der Verbindung $y_1'^2 - 2\, y_2' y_3'$:

$$(\alpha\delta + \beta\gamma)^2 - 4\, \alpha\delta\, \beta\gamma = (\alpha\delta - \beta\gamma)^2,$$

und wir müssen also die Determinante $\alpha\delta - \beta\gamma = \pm 1$ setzen. Berechnet man die Determinante $|A'|$, so ergiebt sich dafür $(\alpha\delta - \beta\gamma)^3$, so dass also, wenn wir nur die eigentlichen orthogonalen Substitutionen berücksichtigen,

$$(13) \qquad \alpha\delta - \beta\gamma = 1$$

setzen müssen, während

$$(14) \qquad \alpha\delta - \beta\gamma = -1$$

den uneigentlichen orthogonalen Substitutionen entspricht. Dadurch ist die Substitution A' völlig bestimmt, und ist zurückgeführt auf die binäre Substitution

$$(15) \qquad (\eta_1, \eta_2) = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} (\xi_1, \xi_2), \quad \alpha\delta - \beta\gamma = \pm 1,$$

oder, wenn $\eta_1 : \eta_2 = \eta$, $\xi_1 : \xi_2 = \xi$ gesetzt wird, auf die lineare gebrochene Substitution

$$(16) \qquad \eta = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}.$$

Hierzu ist aber nun noch Folgendes zu bemerken. Die beiden Substitutionen A, A' sind Transformationen von einander, und entsprechen sich also gegenseitig eindeutig.

Durch A' sind aber die Zahlen $\alpha, \beta, \gamma, \delta$ nur bis auf das gemeinsame Vorzeichen bestimmt. Wenn wir also die lineare Substitution

$$(17) \qquad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

mit einer der beiden Bedingungen (13) und (14) betrachten, so ist zwar hierdurch die Substitution A' und daher auch A eindeutig bestimmt; aber umgekehrt entsprechen jedem A' zwei Substitutionen der Form (17):

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} -\alpha, & -\beta \\ -\gamma, & -\delta \end{pmatrix}.$$

Wir erhalten aber wieder ein eindeutiges Entsprechen, wenn wir diese beiden Substitutionen zu einem gemeinsamen Begriffe, den wir mit A'' bezeichnen, zusammenfassen.

Was nun endlich die Substitution (16) betrifft, die wir mit

$$(18) \qquad A''' = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

bezeichnen, und nach §. 38 als Substitution der Verhältnisse auffassen, so können wir einen gemeinsamen Factor von $\alpha, \beta, \gamma, \delta$

so bestimmen, dass sowohl die Bedingung (13) als (14) befriedigt wird. Demnach bekommen wir aus jeder Substitution A''' zwei orthogonale Substitutionen A, von denen die eine eigentlich, die andere uneigentlich ist.

Die drei Substitutionen

(19) $$A,\ A',\ A''$$

entsprechen sich also hiernach gegenseitig eindeutig, die Substitutionen

(20) $$A,\ A',\ A'''$$

aber nur dann, wenn wir noch die Forderung stellen, dass A eine eigentliche orthogonale Substitution sein soll.

Ist nun

(21) $$B,\ B',\ B''$$

ein zweites System von Substitutionen der Form (19), so sind auch AB, $A'B'$ zwei einander entsprechende Substitutionen, wie unmittelbar aus der Bedeutung der A' als transformirte Substitution der A hervorgeht. Es ist aber noch nachzuweisen, dass auch

(22) $$AB,\ A'B',\ A''B''$$

ein zusammengehöriges System von der Form (19) ist, dass also die Gruppen der A, A', A'' isomorph sind. Daraus ergiebt sich dann von selbst aus der Beziehung, in der A'' und A''' zu einander stehen, dass (bei Beschränkung auf eigentlich orthogonale Substitutionen A) auch die Gruppe der A''' damit isomorph ist.

Setzen wir, um dies zu beweisen:

(23) $$(\eta_1, \eta_2) = A''(\xi_1, \xi_2), \quad (\xi_1, \xi_2) = B''(\zeta_1, \zeta_2),$$

so folgt

(24) $$(\eta_1, \eta_2) = A''B''(\zeta_1, \xi_2).$$

Aus A'', B'', $A''B''$ leiten wir nun nach (12) drei ternäre Substitutionen A', B', C' her. So erhalten wir nach (8):

(25)
$$\begin{aligned}
(\sqrt{2}\,\eta_1\,\eta_2,\ \eta_1^2, \eta_2^2) &= A'\,(\sqrt{2}\,\xi_1\,\xi_2,\ \xi_1^2,\ \xi_2^2)\\
(\sqrt{2}\,\xi_1\,\xi_2,\ \xi_1^2,\ \xi_2^2) &= B'\,(\sqrt{2}\,\zeta_1\,\zeta_2,\ \zeta_1^2,\ \zeta_2^2)\\
(\sqrt{2}\,\eta_1\,\eta_2,\ \eta_1^2, \eta_2^2) &= C'\,(\sqrt{2}\,\zeta_1\,\zeta_2,\ \zeta_1^2,\ \zeta_2^2).
\end{aligned}$$

Diese Formeln sind in Bezug auf ζ_1, ζ_2 identisch, und sie müssen also richtig bleiben, wenn $\sqrt{2}\,\zeta_1\,\zeta_2$, ζ_1^2, ζ_2^2 durch drei

ıabhängige Variable z_1', z_2', z_3' ersetzt werden. Bezeichnen wir e Ausdrücke, die sich dadurch für

$$\sqrt{2}\,\xi_1\,\xi_2,\ \xi_1^2,\ \xi_2^2;\quad \sqrt{2}\,\eta_1\,\eta_2,\ \eta_1^2,\ \eta_2^2$$

'geben, mit

$$x_1',\ x_2',\ x_3';\quad y_1',\ y_2',\ y_3',$$

ergeben die Formeln (25):

6)
$$\begin{aligned}(y_1', y_2', y_3') &= A'(x_1', x_2', x_3')\\ (x_1', x_2', x_3') &= B'(z_1', z_2', z_3')\\ (y_1', y_2', y_3') &= C'(z_1', z_2', z_3'),\end{aligned}$$

h. es ist

$$C' = A'B',$$

z. b. w.

§. 50.

Realitätsbedingungen.

Es bleibt uns noch eine Frage zu beantworten. Bisher haben r nirgends auf die Realität der Coëfficienten Rücksicht ge- ımmen. Wenn aber irgend welche geometrische Anwendung macht werden soll, so ist es nöthig, dass die orthogonale Sub- itution A reell sei. Es ist also noch zu untersuchen, welchen edingungen die Substitutionscoëfficienten $\alpha, \beta, \gamma, \delta$ in A'' zu ıterwerfen sind, damit die Coëfficienten von A reell werden.

Um diese Frage zu entscheiden, bilden wir nach §. 49, (3), (12) e Zusammensetzung

$$A = L A' L^{-1},$$

ıd erhalten:

) $$A = \begin{vmatrix} \alpha\delta + \beta\gamma, & i(\alpha\gamma + \beta\delta), & \alpha\gamma - \beta\delta \\ -i(\alpha\beta + \gamma\delta), & \dfrac{\alpha^2 + \beta^2 + \gamma^2 + \delta^2}{2}, & i\,\dfrac{-\alpha^2 + \beta^2 - \gamma^2 + \delta^2}{2} \\ \alpha\beta - \gamma\delta, & i\,\dfrac{\alpha^2 + \beta^2 - \gamma^2 - \delta^2}{2}, & \dfrac{\alpha^2 - \beta^2 - \gamma^2 + \delta^2}{2} \end{vmatrix}.$$

Die Coëfficienten dieser Substitution sollen also reell sein, ıd ausserdem

) $$\alpha\delta - \beta\gamma = \pm 1.$$

Wenn von den vier Coëfficienten $\alpha, \beta, \gamma, \delta$ einer verschwindet, muss auch noch ein zweiter verschwinden. Denn wenn z. B. $= 0$ ist, so muss $i\alpha\gamma$ und $\alpha\gamma$ reell sein. Dies ist aber mit (2)

nur verträglich, wenn $\gamma = 0$ ist. Ebenso können α und δ nur zugleich verschwinden.

Ist nun β und $\gamma = 0$, so müssen $\alpha^2 + \delta^2$ und $i(\alpha^2 - \delta^2)$ reell sein, also α^2 und δ^2 conjugirt imaginär, und wegen (2) ihr Product $= 1$. Je nachdem also in (2) das obere oder untere Zeichen gilt, müssen $\alpha, \pm \delta$ conjugirt imaginär sein. Ebenso ergiebt sich, dass, wenn α und $\delta = 0$ sind, β und $\mp \gamma$ conjugirt imaginär sein müssen.

Nehmen wir also jetzt an, dass keine der vier Zahlen $\alpha, \beta, \gamma, \delta$ verschwinde. Dann müssen, damit die Grössen

$$\begin{array}{lll} \alpha\delta + \beta\gamma, & i(\alpha\gamma + \beta\delta), & -i(\alpha\beta + \gamma\delta) \\ \alpha\delta - \beta\gamma, & \alpha\gamma - \beta\delta, & \alpha\beta - \gamma\delta \end{array}$$

reell sein können,

$\alpha\delta$ und $\beta\gamma$ reell,
$\alpha\gamma$ conjugirt imaginär mit $-\beta\delta$,
$\alpha\beta$ „ „ „ $-\gamma\delta$

sein, und danach ist auch

$$\alpha^2 = \frac{\alpha\gamma . \alpha\beta}{\beta\gamma} \text{ conjugirt imaginär mit } \delta^2 = \frac{\beta\delta . \gamma\delta}{\beta\gamma}$$

und

$$\beta^2 = \frac{\alpha\beta . \delta\beta}{\alpha\delta} \quad \text{„ „ „} \quad \gamma^2 = \frac{\gamma\delta . \alpha\gamma}{\alpha\delta};$$

also muss α conjugirt mit $\pm \delta$, β conjugirt mit $\mp \gamma$ sein. Dass beide Male das gleiche Zeichen stehe, widerspricht der Forderung, dass $\alpha\gamma$ und $-\beta\delta$ conjugirt sein sollen. Da das Product zweier conjugirt imaginärer Grössen stets positiv ist, so gelten die oberen oder die unteren Zeichen, je nachdem in (2) das obere oder das untere Zeichen steht, d. h. je nachdem A eigentlich oder uneigentlich orthogonal ist. Wir kommen also zu folgendem allgemeinen Resultate, in dem auch die speciellen Fälle von verschwindenden α, β, γ, δ mit enthalten sind:

Die nothwendige und hinreichende Bedingung dafür, dass die orthogonale Substitution (1), (2) reell sei, besteht darin, dass $\alpha, \pm \delta$ und $\beta, \mp \gamma$ zwei conjugirt imaginäre Paare bilden, worin die oberen Zeichen bei den eigentlich, die unteren bei den uneigentlich orthogonalen Substitutionen gelten.

§. 51.

Endliche Gruppen linearer gebrochener Substitutionen. Pole der Gruppen.

Aus den bisherigen Entwickelungen ergiebt sich, dass, wenn alle endlichen Gruppen linearer gebrochener Substitutionen gefunden sind, daraus ohne Weiteres alle endlichen Gruppen eigentlich orthogonaler ternärer Substitutionen und alle endlichen Gruppen binärer linearer Substitutionen mit der Determinante 1 gefunden werden können.

Ausserdem giebt es noch endliche Gruppen, die neben den eigentlichen auch uneigentlich orthogonale Substitutionen enthalten.

Diese Gruppen, auf die wir später zurückkommen, können nicht aus den Gruppen linearer gebrochener Substitutionen allein abgeleitet werden, weil sich bei den gebrochenen Substitutionen der Unterschied zwischen eigentlich und uneigentlich orthogonalen Substitutionen verwischt.

Wir suchen also jetzt zunächst alle endlichen Gruppen linearer gebrochener Substitutionen zu ermitteln[1]).

Wir bezeichnen mit G eine solche Gruppe vom Grade n, und mit

$$(1) \qquad x,\ \Theta_1(x),\ \Theta_2(x), \ldots, \Theta_{n-1}(x)$$

ihre Elemente, worin die Θ Symbole für lineare Functionen

$$(2) \qquad \Theta(x) = \frac{\alpha x + \beta}{\gamma x + \delta}$$

sind, die auch mit

$$(3) \qquad \Theta = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

bezeichnet werden.

Aus jeder Gruppe von der Form (1) können wir nach §. 37 eine ganze Schaar isomorpher Gruppen ableiten, wenn wir mit L eine willkürliche lineare Substitution bezeichnen:

$$(4) \qquad 1,\ L\Theta_1 L^{-1},\ L\Theta_2 L^{-1}, \ldots, L\Theta_{n-1} L^{-1},$$

---

1) Ueber die Theorie dieser Gruppen ist besonders zu vergleichen: Gordan, Ueber endliche Gruppen linearer Transformationen einer Veränderlichen. Mathematische Annalen, Bd. XII, S. 23 (1877); Klein, Vorlesungen über das Ikosaëder (Leipzig 1884).

und wir betrachten unsere Aufgabe als gelöst, wenn von jeder dieser Schaaren ein Repräsentant bestimmt ist.

Wir werden diese Freiheit später benutzen, um die gefundenen Gruppen möglichst einfach darzustellen.

Die Determinante

$$\alpha\delta - \beta\gamma = \Delta$$

muss von Null verschieden sein, und wenn es die Einfachheit verlangt, können wir sie immerhin $= 1$ annehmen, was wir bisweilen thun werden.

Wir bezeichnen im Sinne der Gruppentheorie die Wiederholung einer Substitution durch Exponenten: $\Theta, \Theta^2, \Theta^3, \ldots$, worunter also nicht Potenzen, sondern immer wieder lineare Substitutionen der Gruppe (1) zu verstehen sind. Die identische Substitution $x = x$, die als die Einheit der Gruppe anzusehen ist, wird auch mit Θ^0 oder mit 1 bezeichnet.

Zwei inverse Substitutionen Θ, Θ^{-1} können in der Form dargestellt werden:

$$\Theta = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \quad \Theta^{-1} = \begin{pmatrix} \delta, & -\beta \\ -\gamma, & \alpha \end{pmatrix}.$$

Da die Gruppe nach der Voraussetzung endlich ist, so hat jedes ihrer Elemente einen bestimmten Grad, d. h. es giebt für jedes Θ eine bestimmte kleinste positive Zahl t, für die $\Theta^t = 1$ ist. Diese Zahl t muss ein Theiler von n sein.

Für die Folge ist es von Wichtigkeit, für jede der Substitutionen der Gruppe (ausgenommen die identische Substitution) die Werthe der Variablen zu betrachten, die ihren Transformirten gleich werden, also die Wurzeln der Gleichungen

(5) $$x = \Theta(x).$$

Diese Werthe wollen wir die Pole der Substitution Θ nennen.

Die Gleichung (5) ist quadratisch und nimmt, wenn man für Θ den Ausdruck (2) einsetzt, die Form an:

(6) $$\gamma x^2 + (\delta - \alpha) x - \beta = 0.$$

Diese Gleichung hat zwei Wurzeln, die nur dann einander gleich sind, wenn

(7) $$(\delta - \alpha)^2 + 4\beta\gamma = 0$$

oder

(8) $$(\alpha + \delta)^2 = 4\Delta$$

ist. Es ist leicht einzusehen, dass dieser Fall, wenn Θ einen endlichen Grad hat, nicht vorkommen kann.

Denn ist zunächst β oder $\gamma = 0$, so folgt aus (7), dass $\alpha = \delta$ sein muss, und beide können $= 1$ angenommen werden.

Wenn nun Θ eine der beiden Substitutionen

$$\begin{pmatrix} 1, & 0 \\ \gamma, & 1 \end{pmatrix}, \quad \begin{pmatrix} 1, & \beta \\ 0, & 1 \end{pmatrix}$$

ist, so ist für jedes λ:

$$\Theta^\lambda = \begin{pmatrix} 1, & 0 \\ \lambda\gamma, & 1 \end{pmatrix} \text{ oder } \begin{pmatrix} 1, & \lambda\beta \\ 0, & 1 \end{pmatrix},$$

wie man leicht durch vollständige Induction findet. Es kann also, da β und γ nicht zugleich Null sein können, wenn Θ nicht die identische Substitution ist, Θ^λ für kein positives λ gleich 1 werden, wie es doch sein müsste, wenn λ gleich dem Grade von Θ wäre.

Ist aber β von Null verschieden, so setzen wir, indem wir jetzt $\Delta = 1$ und nach (8) $\alpha + \delta = 2$ annehmen,

$$L = \begin{pmatrix} \beta, & 0 \\ 1 - \alpha, & \beta^{-1} \end{pmatrix},$$

und erhalten

$$L^{-1}\Theta L = \begin{pmatrix} \beta^{-1}, & 0 \\ \alpha - 1, & \beta \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} \beta, & 0 \\ 1 - \alpha, & \beta^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} 1, & \beta^{-1} \\ 0, & 1 \end{pmatrix},$$

also

$$\Theta = L \begin{pmatrix} 1, & \beta^{-1} \\ 0, & 1 \end{pmatrix} L^{-1},$$

und daraus

$$\Theta^\lambda = L \begin{pmatrix} 1, & \lambda\beta^{-1} \\ 0, & 1 \end{pmatrix} L^{-1},$$

was wieder für kein positives λ gleich 1 werden kann. Wir haben daher den Satz:

1. Jede der $n - 1$ nicht identischen Substitutionen einer Gruppe n^{ten} Grades hat zwei von einander verschiedene Pole.

Jede nicht identische Substitution der Gruppe G giebt uns also zwei Pole. Es kann aber ein und derselbe Werth bei mehreren verschiedenen Substitutionen als Pol auftreten. Zählen wir einen dieser Werthe h mal, wenn er in h Substitutionen der Gruppe als Pol vorkommt, so ergiebt sich die Anzahl der Pole

gleich $2n - 2$. Diese Werthe sollen die **Pole der Gruppe** heissen. Die genaue Abzählung dieser Pole giebt uns die wichtigsten Aufschlüsse über Zahl und Beschaffenheit der möglichen endlichen Gruppen.

Wenn die Substitutionscoëfficienten β, γ gleich Null sind, so ist Θ eine multiplicative Substitution

$$\begin{pmatrix} \alpha, & 0 \\ 0, & \delta \end{pmatrix}.$$

Damit diese Substitution von endlichem Grade sein kann, muss der Quotient $\alpha : \delta = \varepsilon$ eine **Einheitswurzel** sein, **deren Grad ein Theiler von** n **ist.** Als Pole dieser Substitution hat man $x = 0$ und $x = \infty$ anzusehen, die der Bedingung

$$x = \varepsilon x$$

genügen.

Nach (4) kann man aus G eine isomorphe Gruppe

$$L G L^{-1} = G'$$

ableiten, wenn für L eine beliebige lineare Substitution

$$L = \begin{pmatrix} A, & B \\ C, & D \end{pmatrix}$$

genommen wird. Die Pole dieser Gruppe erhält man, wenn man auf die Pole von G die Substitution L anwendet. Wenn also a einer der Pole von G ist, so ist

$$a' = \frac{Aa + B}{Ca + D}$$

der entsprechende Pol von G'.

Man kann die Substitutionscoëfficienten A, B, C, D so bestimmen, dass drei der Pole von G' vorgeschriebene Werthe erhalten. Um z. B. den Polen a, b, c von G die Pole $0, \infty, 1$ von G' entsprechen zu lassen, setze man

$$L(x) = \frac{c - b}{c - a} \, \frac{x - a}{x - b}.$$

Wenn a und b die Pole einer und derselben Substitution Θ von G sind, so ist also die entsprechende Substitution von G' multiplicativ.

Wir erhalten hieraus den Satz:

2. **Zu jeder Gruppe linearer Substitutionen kann man eine transformirte Gruppe finden, in der einer beliebigen der gegebenen Substitutionen,**

nur nicht gerade der identischen, eine Multiplication entspricht. Die transformirende Substitution L ist dadurch selbst bis auf eine Multiplication bestimmt.

§. 52.

Die verschiedenen Arten möglicher Gruppen.

Es sei a einer der Pole der Gruppe G, und wir wollen annehmen, es gebe $\nu - 1$ und nicht mehr Elemente in G, $\Theta_1, \Theta_2, \ldots, \Theta_{\nu-1}$, so dass

(1) $$a = \Theta_1(a) = \Theta_2(a) \cdots = \Theta_{\nu-1}(a)$$

ist. Ein solcher Pol soll ein ν-zähliger Pol heissen. Es ist nun zunächst klar, dass die Elemente

(2) $$1, \Theta_1, \Theta_2, \ldots, \Theta_{\nu-1}$$

für sich eine Gruppe, und zwar einen Theiler von G bilden; denn aus

$$a = \Theta_1(a), \; a = \Theta_2(a)$$

folgt, wenn man auf der rechten Seite der zweiten Gleichung a durch das ihm gleiche $\Theta_1(a)$ ersetzt:

$$a = \Theta_2 \Theta_1(a).$$

Es muss also ν ein Theiler von n sein:

(3) $$n = \nu \mu.$$

Wir bezeichnen die Gruppe (2) mit Q.

Es lässt sich beweisen, dass diese Gruppe cyklisch sein muss, also aus den Wiederholungen eines ihrer Elemente besteht.

Denn wenn wir durch Transformation nach dem Satze 2. a nach unendlich werfen, so erhalten die Substitutionen (2) die Form:

$$x, \; \varepsilon_1 x + c_1, \; \varepsilon_2 x + c_2, \ldots, \; \varepsilon_{\nu-1} x + c_{\nu-1},$$

und die Composition von zweien unter ihnen giebt:

$$\begin{aligned} \Theta_1 \Theta_2 &= \varepsilon_1 \varepsilon_2 x + (c_2 \varepsilon_1 + c_1) \\ \Theta^\lambda &= \varepsilon^\lambda x + c\,(\varepsilon^{\lambda-1} + \varepsilon^{\lambda-2} + \cdots + 1) \\ \Theta^{-1} &= \varepsilon^{-1} x - c\,\varepsilon^{-1}. \end{aligned}$$

Daraus schliesst man, dass alle $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ Einheitswurzeln vom Grade ν sein müssen. Ausserdem können nicht zwei der ε einander gleich sein. Denn wäre z. B. $\varepsilon_1 = \varepsilon_2$, so wäre

$$\Theta_1 \Theta_2^{-1} = x + (c_1 - c_2).$$

Diese Substitution muss in G vorkommen und nach dem Satze 1. muss $c_1 = c_2$, also Θ_1 mit Θ_2 identisch sein. Die Zahlen $1, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ müssen also zusammen alle ν^{ten} Einheitswurzeln enthalten, und also mit den Potenzen einer primitiven unter ihnen übereinstimmen. Da andererseits alle Potenzen von einer der Grössen Θ in der Gruppe (1) vorkommen müssen, so wird, wenn das in Θ vorkommende ε eine primitive ν^{te} Einheitswurzel ist, die ganze Gruppe (1) durch die Potenzen von Θ erschöpft. Also besteht diese Gruppe Q aus den Elementen

$$(4) \qquad 1, \Theta, \Theta^2, \ldots, \Theta^{\nu-1}.$$

Nehmen wir (nach dem Satze 2.) Θ als multiplicative Substitution an, so ist 0 der zweite Pol von Θ und zugleich der zweite Pol der sämmtlichen Substitutionen (4). Es ist daher dieser Pol gleichfalls ein mindestens ν-zähliger. Da aber beide Pole von Θ in dieser Betrachtung vertauscht werden können, so erhalten wir die Sätze:

3. Ein ν-zähliger Pol bestimmt eine in G enthaltene cyklische Gruppe Q vom ν^{ten} Grade.
4. Die beiden Pole irgend einer Substitution Θ der Gruppe G sind gleichzählige Pole und sind die beiden einzigen Pole der Gruppe Q.

Nach §. 2 lassen sich $\mu - 1$ Elemente

$$(5) \qquad \psi_1, \psi_2, \ldots, \psi_{\mu-1}$$

in G so auswählen, dass $\psi_1 Q, \psi_2 Q, \ldots, \psi_{\mu-1} Q$ die Nebengruppen zu Q sind, und dass also

$$(6) \qquad G = Q + \psi_1 Q + \psi_2 Q + \cdots + \psi_{\mu-1} Q$$

wird. Wir setzen nun

$$(7) \qquad a_1 = \psi_1(a),\ a_2 = \psi_2(a), \ldots, a_{\mu-1} = \psi_{\mu-1}(a).$$

Die Grössen $a_1, a_2, \ldots, a_{\mu-1}$ sind nicht nur alle von a, sondern auch unter einander verschieden. Denn wäre etwa

$$\psi_1(a) = \psi_2(a),$$

so würde folgen:

$$a = \psi_1^{-1}\psi_1(a) = \psi_1^{-1}\psi_2(a),$$

und $\psi_1^{-1}\psi_2$ wäre in Q enthalten, also ψ_2 in $\psi_1 Q$, was gegen die Voraussetzung ist. Es ist nun leicht nachzuweisen, dass diese Werthe $a_1, a_2, \ldots, a_{\mu-1}$ sämmtlich ν-zählige Pole der Gruppe sind. Es genügt, dies für a_1 zu zeigen.

Wir nehmen irgend eine der Gleichungen (1)

(8) $$a = \Theta(a)$$

und setzen in der Gleichung

(9) $$a_1 = \psi_1(a)$$

für a den ihm gleichen Werth $\Theta(a)$. So erhalten wir

(10) $$a_1 = \psi_1 \Theta(a).$$

Nach (9) ist aber $a = \psi_1^{-1}(a_1)$, und folglich ergiebt sich aus (10):

(11) $$a_1 = \psi_1 \Theta \psi_1^{-1}(a_1).$$

Daraus ersieht man, da wir $\nu - 1$ verschiedene Substitutionen Θ haben, dass a_1 ein ν-zähliger Pol ist und zwar zu der mit Q conjugirten Gruppe $\psi_1 Q \psi_1^{-1}$ gehörig. Aus diesem Grunde nennen wir

(12) $$a, a_1, a_2, \ldots, a_{\mu-1}$$

ein System conjugirter ν-zähliger Pole von G.

Eine beliebige Substitution χ von G kann nach (6) immer in die Form $\psi_i \Theta$ gebracht werden, so dass Θ zu Q gehört, und daraus folgt, dass $\chi(a) = \psi_i \Theta(a) = a_i$ ist, und ebenso, wenn man $\psi_i \Theta \psi_k = \psi_h \Theta'$ setzt, so dass auch Θ' zu Q gehört:

$$\chi(a_k) = \psi_i \Theta \psi_k(a) = \psi_h \Theta'(a) = a_h.$$

Da ferner zwei Grössen $\chi(a_h)$, $\chi(a_k)$ nur dann einander gleich sein können, wenn $a_h = a_k$ ist, so folgt der Satz:

5. Die beiden Reihen

$$a, \quad a_1, \quad a_2, \quad \ldots, \quad a_{\mu-1}$$
$$\chi(a), \chi(a_1), \chi(a_2), \ldots, \chi(a_{\mu-1})$$

stimmen, welche Substitution aus G auch für χ genommen werden mag, abgesehen von der Reihenfolge, mit einander überein.

Ist dann b ein in dem Systeme (12) nicht enthaltener Pol, so kann auch $\chi(b)$ nicht in (12) vorkommen, und daraus ergiebt sich, dass zwei Systeme conjugirter Pole, wenn sie nicht ganz identisch sind, keinen Pol gemein haben.

Hiernach können wir die sämmtlichen Pole der Gruppe G in Systeme conjugirter Pole anordnen, und wir erhalten nach §. 51 ihre Gesammtzahl $2n - 2$, wenn wir jeden ν-zähligen Pol $(\nu - 1)$mal mitrechnen.

Diese Bemerkung giebt uns eine wesentliche Begrenzung der Zahlen ν. Es ist nämlich danach:

(13) $$2n-2 = \mu(\nu-1) + \mu'(\nu'-1) + \mu''(\nu''-1) + \cdots$$

oder, wenn wir mit h die Anzahl der Systeme conjugirter Pole bezeichnen, und $n = \mu\nu = \mu'\nu' = \cdots$ setzen:

(14) $$2n-2 = nh - \mu - \mu' - \mu'' - \cdots$$

Die Zahlen $\nu, \nu', \nu'' \ldots$ sind mindestens gleich 2, also ist

$$1 \leqq \mu \leqq \frac{n}{2}, \quad 1 \leqq \mu' \leqq \frac{n}{2}, \cdots$$

und daher nach (14)

$$\frac{nh}{2} \leqq 2n-2 \leqq (n-1)h,$$

oder

$$2 \leqq h \leqq 4 - \frac{4}{n}.$$

Es kann also h nur einen der beiden Werthe 2 oder 3 haben, und wir finden fünf Arten, die Gleichung (13) zu befriedigen.

Wenn zunächst $h = 2$ ist, so folgt aus (14)

$$\mu + \mu' = 2, \quad \mu = \mu' = 1, \quad \nu = \nu' = n.$$

Wir haben also:

I. Kreistheilungsgruppe oder cyklische Gruppe:
$\nu = \nu' = n$, n beliebig.
$\mu = \mu' = 1$,

Ist ferner $h = 3$, so folgt aus (14):

(15) $$\mu + \mu' + \mu'' = n + 2.$$

Daraus ist zu schliessen, dass mindestens eine der Zahlen ν, ν', ν'' gleich 2 sein muss. Denn wären sie alle $\geqq 3$, so wäre

$$\mu \leqq \frac{n}{3}, \quad \mu' \leqq \frac{n}{3}, \quad \mu'' \leqq \frac{n}{3},$$

also $\mu + \mu' + \mu'' \leqq n$, was mit (15) im Widerspruch steht.

Ist also $\nu = 2$, $\mu = \frac{n}{2}$, so folgt aus (15):

(16) $$\mu' + \mu'' = \frac{n}{2} + 2.$$

Wir nehmen zunächst an, dass auch noch $\nu' = 2$ sei. Setzen wir dann $\nu'' = m$, so folgt aus (16):

$$\mu'' = 2, \quad n = 2m,$$

und wir erhalten eine zweite Möglichkeit:

II. Diëdergruppe, $\nu = \nu' = 2$, $\nu'' = m$, $n = 2m$, $m \gtreqless 2$
$\mu = \mu' = m$, $\mu'' = 2$.

Ist ferner keine der Zahlen ν', ν'' gleich 2, so muss eine von ihnen gleich 3 sein. Denn sind sie beide $\gtreqless 4$, so ist

$$\mu' + \mu'' \lesseqgtr \frac{n}{2},$$

was mit (16) im Widerspruche steht. Ist also $\nu' = 3$, $\mu' = \frac{n}{3}$, so folgt aus (16):

$$(17) \qquad \mu'' = \frac{n}{6} + 2, \quad \nu'' = \frac{6n}{n+12},$$

woraus folgt, dass $\nu'' < 6$ sein muss, also nur einen der Werthe 3, 4, 5 haben kann.

Danach bekommen wir noch drei mögliche Fälle:

III. Tetraëdergruppe: $\nu = 2$, $\nu' = 3$, $\nu'' = 3$, $n = 12$
$\mu = 6$, $\mu' = 4$, $\mu'' = 4$.

IV. Octaëdergruppe: $\nu = 2$, $\nu' = 3$, $\nu'' = 4$, $n = 24$
$\mu = 12$, $\mu' = 8$, $\mu'' = 6$.

V. Ikosaëdergruppe: $\nu = 2$, $\nu' = 3$, $\nu'' = 5$, $n = 60$
$\mu = 30$, $\mu' = 20$, $\mu'' = 12$.

Hiermit sind alle Möglichkeiten erschöpft.

Es ist freilich noch nicht bewiesen, dass diese Gruppen, die wir einstweilen mit den gebräuchlichen Namen aufgeführt haben, und die wir unter dem gemeinsamen Namen der Polyëdergruppen zusammenfassen, wirklich existiren, noch wie gross ihre Mannigfaltigkeit ist. Zu diesem Beweise führen erst die folgenden Betrachtungen.

§. 53.

Transformation der Substitutionen von G auf einfache Formen.

Ehe wir zur definitiven Aufstellung dieser Gruppen gehen, leiten wir einen Satz ab, der die Möglichkeit der vorkommenden Substitutionen noch weiter beschränkt.

Ist a ein ν-zähliger Pol der Gruppe G und

(1) $$a = \Theta(a) = \Theta^2(a) \cdots = \Theta^{\nu-1}(a),$$

so ist der zweite Pol a' von Θ nach §. 52, 4. gleichfalls ν-zählig, und es ist

(2) $$a' = \Theta(a') = \Theta^2(a') \cdots = \Theta^{\nu-1}(a').$$

Giebt es nun in der Gruppe G mehr als ein System conjugirter ν-zähliger Pole, so können a, a' entweder in demselben oder auch in verschiedenen dieser Systeme vorkommen.

Giebt es aber nur ein System ν-zähliger Pole, so muss a und a' in demselben Systeme vorkommen, und es muss also in G eine nicht unter den Potenzen von Θ enthaltene Substitution ψ existiren, so dass

(3) $$a' = \psi(a)$$

ist. Daraus folgt mit Anwendung von (1) und (2):

$$\psi(a) = \Theta\psi(a), \quad a = \psi^{-1}\Theta\psi(a),$$

woraus zu schliessen ist, dass $\psi^{-1}\Theta\psi$ unter den Potenzen von Θ vorkommt, und dass daher nach (2) auch

$$a' = \psi^{-1}\Theta\psi(a'), \quad \psi(a') = \Theta\psi(a')$$

sein muss. Es ist also auch $\psi(a')$ ein Pol von Θ, und weil $\psi(a')$ nicht $= a'$ sein kann, weil sonst a' ein Pol von ψ wäre, was nicht sein kann, da ψ nicht unter den Potenzen von Θ vorkommt, so ist

(4) $$\psi(a') = a.$$

Wenn man nun durch Transformation der Gruppe die Pole a und a' nach 0 und ∞ bringt, so erhält Θ die Form

$$\Theta(x) = \varepsilon x,$$

worin ε eine primitive ν^{te} Einheitswurzel ist, und ψ muss wegen (3) und (4) die Form haben:

$$\psi(x) = \frac{c}{x},$$

worin c eine Constante ist. Durch eine abermalige Transformation der Gruppe kann man der Constanten c jeden beliebigen Werth, z. B. durch Transformation mit der Substitution $x\sqrt{c}$ für x, den Werth 1 geben. Wir erhalten also folgenden Satz:

1. Wenn in der Gruppe G nur ein System conjugirter ν-zähliger Pole vorkommt, so kann man

die Gruppe so transformiren, dass sie die beiden Substitutionen

$$\Theta = \varepsilon x, \quad \psi = \frac{c}{x}$$

enthält, worin ε eine primitive ν^{te} Einheitswurzel bedeutet, und c ein beliebig vorgeschriebener Werth, z. B. auch 1, sein kann.

Die Voraussetzung dieses Satzes ist bei den in §. 52 aufgezählten Fällen immer für einen der verschiedenen Werthe ν erfüllt, ausgenommen bei der cyklischen Gruppe und bei der Diëdergruppe mit $m = 2$.

Endlich beweisen wir noch den folgenden Satz:

2. Sind a, a' die Pole einer Substitution Θ von G, so sind die mit a und a' conjugirten Pole

$$b = \chi(a), \quad b' = \chi(a'),$$

worin χ eine beliebige Substitution aus G ist, die beiden Pole einer und derselben Substitution, nämlich der Substitution $\chi\Theta\chi^{-1}$.

Die Richtigkeit ergiebt sich unmittelbar aus dem Anblick der Gleichungen:

$$a = \Theta(a), \quad \chi\Theta\chi^{-1}\chi(a) = \chi\Theta(a) = \chi(a)$$
$$a' = \Theta(a'), \quad \chi\Theta\chi^{-1}\chi(a') = \chi\Theta(a') = \chi(a').$$

§. 54.

Die Grundformen.

Um zu der endgültigen Aufstellung aller endlichen Gruppen G zu gelangen, ist es nothwendig, auf die Invarianten der entsprechenden binären Substitutionsgruppen näher einzugehen.

Wir müssen daher neben den linearen gebrochenen Substitutionen

$$(1) \qquad y = \frac{\alpha x + \beta}{\gamma x + \delta},$$

die wir im §. 49 mit A''' bezeichnet haben, noch die binären Substitutionen

$$(2) \qquad (y_1, y_2) = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} (x_1, x_2)$$

betrachten, die dort mit A'' bezeichnet waren, und die, wenn man $y_1 : y_2 = y$, $x_1 : x_2 = x$ setzt, wieder auf die Substitution (1) führen. In (2) ist immer

$$(3) \qquad \alpha\delta - \beta\gamma = 1$$

vorausgesetzt, aber die beiden Substitutionen

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \quad \begin{pmatrix} -\alpha, & -\beta \\ -\gamma, & -\delta \end{pmatrix}$$

werden als identisch angesehen.

Es kann nicht zu einem Missverständniss führen, wenn wir beide Arten von Substitutionen übereinstimmend durch ein Symbol wie

$$\Theta = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

bezeichnen, da ja dann in beiden die Compositionsregel genau dieselbe ist.

Wenn nun

$$(4) \qquad a, a_1, a_2, \ldots, a_{\mu-1}$$

ein System conjugirter Pole der Gruppe G ist, so ist

$$(5) \qquad f(x) = (x - a)(x - a_1) \ldots (x - a_{\mu-1})$$

eine ganze Function μ^{ten} Grades, deren Wurzeln jene conjugirten Pole sind. Diese Function $f(x)$ hat folgende Eigenschaft:

Nehmen wir irgend eine Substitution der Gruppe G

$$\psi(x) = \frac{\alpha x + \beta}{\gamma x + \delta},$$

so sind die Wurzeln der Function

$$(6) \qquad (\gamma x + \delta)^{\mu} f[\psi(x)]$$

die Grössen $\psi^{-1}(a)$, $\psi^{-1}(a_1)$, ..., $\psi^{-1}(a_{\mu-1})$. Diese aber stimmen, von der Reihenfolge abgesehen, nach §. 52, 5. mit den Grössen $a, a_1, a_2, \ldots, a_{\mu-1}$ überein, und folglich können sich die Gleichungen (5) und (6) nur durch einen constanten Factor unterscheiden. Wenn wir also

$$(7) \qquad x_2^{\mu} f\left(\frac{x_1}{x_2}\right) = f(x_1, x_2)$$

setzen, so bleibt diese Form f, von einem constanten Factor abgesehen, ungeändert, wenn auf (x_1, x_2) irgend eine Substitution der Gruppe G angewandt wird.

Nach der Definition §. 40, 2. ist also $f(x_1, x_2)$ eine Invariante der Gruppe G, und wir haben den Satz:

1. **Jedem Systeme conjugirter Pole der Gruppe G entspricht eine invariante Form, deren Grad gleich der Anzahl der Pole des Systemes ist, und deren Wurzeln eben diese Pole sind.**

Wir bezeichnen mit $f_1, f_2, \ldots$ die zu den verschiedenen Systemen conjugirter Pole gehörigen invarianten Formen, die von den Graden $\mu, \mu', \ldots$ sind und die wir die **Grundformen** der Gruppe nennen wollen.

Ist dann $F(x_1, x_2)$ **irgend** eine invariante Form der Gruppe G und $f(x, y)$ eine Grundform, und hat $F(x, 1) = 0$ mit $f(x, 1) = 0$ eine gemeinsame Wurzel, so müssen alle Wurzeln von $f = 0$ zugleich Wurzeln von $F = 0$ sein. Denn nach Voraussetzung haben die beiden Functionen $F(x, 1)$ und $F[\psi(x), 1]$ dieselben Wurzeln. Wenn also $F(a, 1) = 0$ ist, so ist auch $F[\psi(a), 1] = F(a_1, 1) = 0$. Wir haben also den folgenden Satz:

2. **Hat eine zu G gehörige invariante Form $F(x_1, x_2)$ mit einer der Grundformen $f(x_1, x_2)$ einen Theiler gemein, so ist $F(x_1, x_2)$ durch $f(x_1, x_2)$ theilbar.**

Ist $F(x_1, x_2)$ eine invariante Form der Gruppe G, und ξ eine Wurzel der Gleichung $F(x, 1) = 0$, so sind auch, wenn ψ die Elemente der Gruppe G durchläuft, die sämmtlichen n Grössen $\psi(\xi)$ Wurzeln derselben Gleichung. Wenn also der Grad von F niedriger ist, als der Grad der Gruppe, so können diese Grössen nicht alle von einander verschieden sein, und es folgt für irgend zwei von einander verschiedene Substitutionen χ, ψ von G

$$\chi(\xi) = \psi(\xi)$$

oder

$$\xi = \chi^{-1}\psi(\xi),$$

d. h. ξ muss unter den Polen der Gruppe G vorkommen, und es ist also F nach dem Satze 2. durch eine der Grundformen theilbar. Da wir auf den Quotienten der Division dieselbe Schlussweise anwenden können, so folgt:

3. **Eine invariante Form F der Gruppe G, deren Grad niedriger ist, als der Grad der Gruppe, ist, von einem constanten Factor abgesehen, ein Product von Potenzen der Grundformen.**

Es ist hierbei immer angenommen, dass die Coëfficienten von $F(x_1, x_2)$ nicht alle gleich Null sind. Wir können also, wenn wir von dieser Voraussetzung absehen, den Satz 3. auch so aussprechen:

4. Ist $F(x_1, x_2)$ eine invariante Form der Gruppe G von niedrigerem Grade als G, die sich nicht als Product aus den Grundformen darstellen lässt, so muss $F(x_1, x_2)$ identisch verschwinden.

Achter Abschnitt.

Die Polyëdergruppen.

---

§. 55.

Die cyklischen Gruppen und die Diëdergruppen.

Wir gehen nun dazu über, die allgemeinen Principien zur wirklichen Bildung der verschiedenen Polyëdergruppen anzuwenden, zunächst also zu zeigen, dass die in §. 52 als möglich erkannten Arten dieser Gruppen alle existiren.

Bei den cyklischen Gruppen n^{ten} Grades haben wir nur zwei Systeme conjugirter Pole, deren jedes nur einen $(n-1)$fachen Pol enthält. Diese beiden Pole müssen also die gemeinsamen Pole aller Substitutionen der Gruppe sein und können nach §. 51, 2. als 0 und ∞ angenommen werden. Wir haben dann nur die beiden linearen Grundformen

(1) $$f_1 = x_1, \quad f_2 = x_2.$$

Alle Substitutionen der Gruppe sind multiplicativ, und der Multiplicator muss eine n^{te} Einheitswurzel sein. Sie müssen also die Form haben:

(2) $$x, \ \varepsilon x, \ \varepsilon^2 x, \ldots, \ \varepsilon^{n-1} x,$$

wenn ε eine primitive n^{te} Einheitswurzel ist.

Wir erhalten also in der That für jedes n eine cyklische Gruppe, die wir mit C_n bezeichnen wollen:

(3) $$C_n = \begin{pmatrix} \varepsilon^r, & 0 \\ 0, & 1 \end{pmatrix}, \quad r = 0, 1, \ldots, n-1,$$

oder mit der Determinante 1 geschrieben:

(4) $$C_n = \begin{pmatrix} \varepsilon^{\frac{1}{2}r}, & 0 \\ 0, & \varepsilon^{-\frac{1}{2}r} \end{pmatrix}.$$

Bei der Diëdergruppe vom Grade $n = 2m$, die wir mit D_m bezeichnen wollen, haben wir nach dem vorigen Paragraphen zwei Systeme von je m conjugirten zweizähligen Polen und ein System von zwei conjugirten m-zähligen Polen. Die letzteren müssen also nach dem Satze §. 53 die Pole einer Substitution sein. Wenn wir sie mit 0 und ∞ zusammenfallen lassen, so erhalten wir die Grundform zweiten Grades:

$$f_1 = x_1 x_2.$$

Dies kann aber nur dann eine invariante Form der Gruppe sein, wenn alle Substitutionen in einer der beiden Formen

$$\begin{pmatrix} \alpha, & 0 \\ 0, & \delta \end{pmatrix}, \quad \begin{pmatrix} 0, & \beta \\ \gamma, & 0 \end{pmatrix}$$

enthalten sind, und hierin müssen $\alpha : \delta$ und $-\beta : \gamma$ m^{te} Einheitswurzeln sein. Wir bekommen also die Substitutionen der Gruppe, wenn ε eine primitive m^{te} Einheitswurzel ist:

$$x, \ \varepsilon x, \ \varepsilon^2 x, \ldots, \varepsilon^{m-1} x$$

$$\frac{1}{x}, \ \frac{\varepsilon}{x}, \ \frac{\varepsilon^2}{x}, \ldots, \frac{\varepsilon^{m-1}}{x},$$

d. h.

(5) $$D_m = \begin{pmatrix} \varepsilon^r, & 0 \\ 0, & 1 \end{pmatrix}, \ \begin{pmatrix} 0, & \varepsilon^r \\ 1, & 0 \end{pmatrix},$$

oder, mit der Determinante $+1$ dargestellt:

(6) $$D_m = \begin{pmatrix} \varepsilon^{\frac{1}{2}r}, & 0 \\ 0, & \varepsilon^{-\frac{1}{2}r} \end{pmatrix}, \ \begin{pmatrix} 0, & i\,\varepsilon^{\frac{1}{2}r} \\ i\,\varepsilon^{-\frac{1}{2}r}, & 0 \end{pmatrix}, \ r = 0, 1, \ldots, m-1.$$

Man sieht sofort, dass diese Substitutionen wirklich eine Gruppe bilden.

Ausser 0 und ∞ haben wir hier noch die aus den Gleichungen

$$x = \frac{\varepsilon^h}{x}$$

hervorgehenden Pole $\pm\, \varepsilon^{\frac{1}{2}h}$, aus denen man noch die beiden Grundformen m^{ten} Grades

(7) $$f_2 = x_1^m + x_2^m, \quad f_3 = x_1^m - x_2^m$$

erhält.

Hieraus ersieht man, dass die Diëdergruppen und die cyklischen Gruppen ganz von einander verschieden sind, da ihre Grundformen verschiedene Grade haben.

Durch Transformation mittelst der Substitution

$$\begin{pmatrix} e^{\frac{\pi i}{4}}, & 0 \\ 0, & e^{-\frac{\pi i}{4}} \end{pmatrix}$$

geht die Diëdergruppe D_m in

$$\begin{pmatrix} \varepsilon^{1/2\lambda}, & 0 \\ 0, & \varepsilon^{-1/2\lambda} \end{pmatrix}, \quad \begin{pmatrix} 0, & \varepsilon^{1/2\lambda} \\ -\varepsilon^{-1/2\lambda}, & 0 \end{pmatrix}$$

oder in

$$x, \quad \varepsilon x, \quad \varepsilon^2 x, \quad \ldots, \quad \varepsilon^{m-1} x$$

$$\frac{-1}{x}, \quad \frac{-\varepsilon}{x}, \quad \frac{-\varepsilon^2}{x}, \quad \ldots, \quad \frac{-\varepsilon^{m-1}}{x}$$

über, und die Grundformen für diese Darstellung sind:

$$f_1 = x_1 x_2, \quad f_2 = x_1^m + i^m x_2^m, \quad f_3 = x_1^m - i^m x_2^m.$$

Die Diëdergruppe D_m enthält als Theiler die cyklische Gruppe C_m, und zwar ist C_m ein Normaltheiler von D_m.

Durch Transformation mit irgend einer multiplicativen Substitution

$$\begin{pmatrix} \alpha, & 0 \\ 0, & \delta \end{pmatrix}$$

ändert sich C_m nicht, während die nicht in C_m enthaltenen Substitutionen von D_m ihre Form ändern; denn es ist:

$$\begin{pmatrix} \delta, & 0 \\ 0, & \alpha \end{pmatrix} \begin{pmatrix} \varepsilon, & 0 \\ 0, & 1 \end{pmatrix} \begin{pmatrix} \alpha, & 0 \\ 0, & \delta \end{pmatrix} = \begin{pmatrix} \varepsilon, & 0 \\ 0, & 1 \end{pmatrix},$$

$$\begin{pmatrix} \delta, & 0 \\ 0, & \alpha \end{pmatrix} \begin{pmatrix} 0, & \varepsilon \\ 1, & 0 \end{pmatrix} \begin{pmatrix} \alpha, & 0 \\ 0, & \delta \end{pmatrix} = \begin{pmatrix} 0, & \varepsilon\,\delta^2 \\ \alpha^2, & 0 \end{pmatrix}.$$

Abgesehen von einer solchen multiplicativen Substitution ist aber die Gruppe D_m durch die darin enthaltene Gruppe C_m vollkommen bestimmt. Denn setzen wir

$$D_m = C_m +. \varphi\, C_m,$$

worin

$$\varphi = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

gesetzt ist, so muss, da C_m Normaltheiler von D_m sein muss, $\varphi\, C_m = C_m\, \varphi$ sein, d. h. es muss sich zu jedem Exponenten r ein Exponent s, und umgekehrt, bestimmen lassen, so dass

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} \varepsilon^r, & 0 \\ 0, & 1 \end{pmatrix} = \begin{pmatrix} \varepsilon^s, & 0 \\ 0, & 1 \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

oder

$$\begin{pmatrix}\alpha\varepsilon^r, & \beta \\ \gamma\varepsilon^r, & \delta\end{pmatrix} = \begin{pmatrix}\varepsilon^s\alpha, & \varepsilon^s\beta \\ \gamma, & \delta\end{pmatrix}.$$

Wären β und $\gamma = 0$, so wäre φ selbst von der Form εx, und ε eine $2m^{\text{te}}$ Einheitswurzel, und D_m wäre also eine cyklische Gruppe und keine Diëdergruppe. Ist aber β oder γ von Null verschieden, so folgt $\varepsilon^s = \varepsilon^{-r}$ und $\alpha = \delta = 0$, also

$$\varphi = \begin{pmatrix}0, & \beta \\ \gamma, & 0\end{pmatrix},$$

was durch eine multiplicative Transformation auf die Form $\begin{pmatrix}0, & 1 \\ 1, & 0\end{pmatrix}$ gebracht werden kann.

Unter den Diëdergruppen ist die Gruppe D_2 besonders hervorzuheben, in der drei Systeme von je zwei zweizähligen Polen vorhanden sind. Sie besteht aus den vier Substitutionen

$$\begin{pmatrix}1, & 0 \\ 0, & 1\end{pmatrix}, \begin{pmatrix}-1, & 0 \\ 0, & 1\end{pmatrix}, \begin{pmatrix}0, & 1 \\ 1, & 0\end{pmatrix}, \begin{pmatrix}0, & 1 \\ -1, & 0\end{pmatrix}$$

und wird die Vierergruppe genannt.

§. 56.

Die Tetraëdergruppe.

Bei der Tetraëdergruppe haben wir nach §. 52, III. ein System von sechs conjugirten zweizähligen Polen. Wir können also nach §. 53 annehmen, dass in der Gruppe die beiden Substitutionen

$$\Theta(x) = -x, \quad \psi(x) = \frac{1}{x}$$

vorkommen, und folglich auch

$$\psi_1(x) = \psi\,\Theta(x) = -\frac{1}{x}.$$

Die beiden Substitutionen ψ und ψ_1 geben die Pole ± 1 und $\pm i$, und diese müssen, da ψ und ψ_1 vom 2ten Grade sind und in G überhaupt nur zwei- oder dreizählige Pole vorkommen, zu den zweizähligen gehören (§. 52, 3.). Die Substitution $\Theta(x)$ giebt die zweizähligen Pole $0, \infty$. Demnach lautet die Gleichung, von der die zweizähligen Pole abhängen, $x(x^4 - 1) = 0$ und wir erhalten die erste Grundform 6ten Grades:

(1) $$f(x_1, x_2) = x_1 x_2 (x_1^4 - x_2^4).$$

Um die übrigen Substitutionen der Gruppe zu finden, bemerken wir, dass wir nach dem Theorem §. 53, 2., wenn wir ± 1 für a, a' und $0, \infty$ für b, b' nehmen, auf die Existenz einer Substitution χ in G schliessen können, die den Bedingungen genügt

$$\chi(-1) = 0, \quad \chi(+1) = \infty,$$

und dass also χ die Form haben muss:

$$\chi = \lambda \frac{x+1}{x-1}, \tag{2}$$

wo λ ein constanter Factor ist.

Wenn wir in χ die sechs conjugirten Pole $0, \infty, +1, -1, +i, -i$ einsetzen, so müssen wir dieselben Werthe in einer anderen Reihenfolge erhalten (§. 52, 5.). Diese Werthe sind aber

$$-\lambda, \ \lambda, \ \infty, \ 0, \ -\lambda i, \ \lambda i.$$

Es muss also $\lambda = \pm 1$ oder $= \pm i$ sein. Der Werth ± 1 ist nicht zulässig, weil sonst

$$\chi(i) = \mp i, \quad \Theta\chi(i) = \pm i,$$

und also $\pm i$ die Pole von χ oder von $\Theta\chi$ wären, während sie doch nur zweizählig und die Pole von $\Theta\psi$ sind. Es muss also $\lambda = \pm i$ sein, und wir können ohne Beschränkung der Allgemeinheit das obere Zeichen nehmen, denn das untere Zeichen entspricht dann der Substitution $\Theta\chi$. Es ist daher

$$\chi(x) = i \frac{x+1}{x-1}.$$

Daraus erhält man

$$\chi^2(x) = \frac{x+i}{x-i}, \quad \chi^3(x) = x,$$

und es ergeben sich die 12 Substitutionen:

$$\begin{array}{llll} 1, & \Theta, & \psi, & \Theta\psi \\ \chi, & \Theta\chi, & \psi\chi, & \Theta\psi\chi \\ \chi^2, & \Theta\chi^2, & \psi\chi^2, & \Theta\psi\chi^2, \end{array} \tag{3}$$

oder

$$\pm x, \ \pm \frac{1}{x}, \ \pm i \frac{x+1}{x-1}, \ \pm i \frac{x-1}{x+1}, \ \pm \frac{x+i}{x-i}, \ \pm \frac{x-i}{x+i}. \tag{4}$$

Dass diese Substitutionen wirklich eine Gruppe, die **Tetraëdergruppe**, bilden, von der Θ, ψ, χ die erzeugenden Elemente sind, ergiebt sich aus

$$\chi\Theta = \Theta\psi\chi, \ \chi^2\Theta = \psi\chi^2, \ \psi\Theta = \Theta\psi, \ \chi\psi = \Theta\chi, \ \chi^2\psi = \Theta\psi\chi^2, \tag{5}$$

die sich mit Rücksicht auf $\Theta^2 = \psi^2 = \chi^3 = 1$ aus den drei Relationen

$$\psi\Theta = \Theta\psi, \quad \chi\Theta = \Theta\psi\chi, \quad \chi\psi = \Theta\chi$$

ableiten lassen.

Aus (5) geht noch hervor, dass die Vierergruppe

$$(6) \qquad 1, \Theta, \psi, \Theta\psi$$

ein Normaltheiler der Tetraëdergruppe ist.

Die Substitutionen der Tetraëdergruppe können in jeder der beiden Formen

$$\chi^\lambda \psi^\mu \Theta^\nu, \quad \Theta^\nu \psi^\mu \chi^\lambda$$

$$\lambda = 0, 1, 2, \quad \mu = 0, 1, \quad \nu = 0, 1$$

dargestellt werden.

Um die zu den dreizähligen Polen gehörigen beiden Grundformen vierter Ordnung Φ_1, Φ_2 zu erhalten, kann man entweder aus (5) die noch fehlenden Pole berechnen, oder man kann so verfahren:

Da die Grundformen Φ_1, Φ_2 die Substitutionen Θ und ψ gestatten müssen und nicht durch x_1 und x_2 theilbar sein können, so können sie nur von folgender Form sein:

$$\Phi_1 = x_1^4 + m_1 x_1^2 x_2^2 + x_2^4$$
$$\Phi_2 = x_1^4 + m_2 x_1^2 x_2^2 + x_2^4,$$

worin m_1, m_2 noch zu bestimmende Constanten sind. Bildet man aber die Hesse'sche Covariante von Φ_1, so erhält man nach §. 40, 4. eine Invariante der Gruppe:

$$\frac{1}{12}\left[\frac{\partial^2 \Phi_1}{\partial x_1^2}\frac{\partial^2 \Phi_1}{\partial x_2^2} - \left(\frac{\partial^2 \Phi_1}{\partial x_1 \partial x_2}\right)^2\right] = 2 m_1 (x_1^4 + x_2^4) + (12 - m_1^2) x_1^2 x_2^2.$$

Diese Form kann, da keine anderen Grundformen vierter Ordnung existiren, nur entweder mit Φ_1 oder mit Φ_2 übereinstimmen (von einem constanten Factor abgesehen). Es muss also

$$\frac{12 - m_1^2}{2 m_1} = m_1 \text{ oder } m_2$$

sein. Die erste Annahme giebt aber $m_1 = \pm 2$. Dann wäre Φ_1 ein Quadrat, was nicht sein kann. Es bleibt also nur:

$$m_1^2 + 2 m_1 m_2 = 12,$$

und ebenso aus Φ_2:

$$m_2^2 + 2 m_1 m_2 = 12,$$

also

$$m_1 = - m_2 = \pm 2\sqrt{-3},$$

und die beiden Grundformen werden:

$$(7)\qquad \begin{aligned} \Phi_1 &= x_1^4 + 2\sqrt{-3}\; x_1^2 x_2^2 + x_2^4 \\ \Phi_2 &= x_1^4 - 2\sqrt{-3}\; x_1^2 x_2^2 + x_2^4. \end{aligned}$$

Zwischen den drei Grundformen f, Φ_1, Φ_2 kann man eine Relation herleiten, wenn man x_1, x_2 eliminirt. Man findet aus (7)

$$2\,(x_1^4 + x_2^4) = \Phi_1 + \Phi_2$$

$$4\sqrt{-3}\; x_1^2 x_1^2 = \Phi_1 - \Phi_2,$$

und aus (1)

$$f^2 = x_1^2 x_2^2 (x_1^4 + x_2^4)^2 - 4\, x_1^6 x_2^6,$$

woraus man leicht berechnet

$$(8)\qquad 12\sqrt{-3}\, f^2 = \Phi_1^3 - \Phi_2^3.$$

Die Substitutionen Θ, ψ, χ erhalten, wenn sie mit der Determinante 1 dargestellt werden, den Ausdruck:

$$(9)\qquad \begin{pmatrix} i, & 0 \\ 0, & -i \end{pmatrix}, \quad \begin{pmatrix} 0, & i \\ i, & 0 \end{pmatrix}, \quad \begin{pmatrix} \frac{1-i}{2}, & \frac{1-i}{2} \\ -\frac{1+i}{2}, & \frac{1+i}{2} \end{pmatrix},$$

woraus nach den im §. 50 aufgestellten Bedingungen folgt, dass die entsprechende Gruppe orthogonaler ternärer Substitutionen reell ist.

Wendet man die Substitutionen (9) mit der Determinante 1 auf die Grundform $f(x_1, x_2)$ an, so ergiebt eine sehr einfache Rechnung, dass die Grundform f eine absolute Invariante der binären Gruppe G ist.

Dieselbe Eigenschaft hat auch die Hesse'sche Determinante von f:

$$\begin{aligned} H &= -\frac{1}{25}\,[f''(x_1, x_1)\, f''(x_2, x_2) - f''(x_1, x_2)^2] \\ &= (x_1^4 + x_2^4)^2 + 12\, x_1^4\, x_2^4, \end{aligned}$$

die nichts Anderes ist, als das Product der beiden Functionen Φ_1, Φ_2; während die Functionen Φ_1 und Φ_2 selbst bei der dritten der Substitutionen (9) eine dritte Einheitswurzel als Factor annehmen.

§. 57.

Die Octaëdergruppe.

Bei der Octaëdergruppe kommt ein System von sechs conjugirten vierzähligen Polen vor. Wir haben demnach eine Substitution 4ten Grades, deren Periode

$$1,\ \Theta,\ \Theta^2,\ \Theta^3,\quad \Theta^4 = 1$$

ein Paar dieser conjugirten vierzähligen Pole giebt. Nach §. 53, 1. können wir in der Gruppe die Substitutionen annehmen:

(1) $$\Theta(x) = i\,x,\quad \psi(x) = \frac{1}{x},$$

und es ist

(2) $$\psi^2 = 1,\quad \Theta\psi = \psi\Theta^3,\quad \Theta^2\psi = \psi\Theta^2,\quad \Theta^3\psi = \psi\Theta.$$

Die zu dem Systeme der vierzähligen Pole gehörige Grundform 6ten Grades muss bis auf einen constanten Factor ungeändert bleiben durch die Substitutionen Θ und ψ, und sie muss ausserdem den Factor $x_1\, x_2$ enthalten, also von einer der beiden Formen sein

$$x_1\, x_2\,(x_1^4 - x_2^4),\quad x_1\, x_2\,(x_1^4 + x_2^4).$$

Es ist gleichgültig, welche der beiden Annahmen wir verfolgen, da die eine durch die Substitution $i\,x_2$ für x_2, was dem Uebergange zu einer transformirten Gruppe entspricht, in die andere übergeht. Nehmen wir

(3) $$f(x_1, x_2) = x_1\, x_2\,(x_1^4 - x_2^4)$$

als Grundform 6ten Grades an, so sind die sechs vierzähligen Pole

(4) $$0,\ \infty,\ 1,\ -1,\ i,\ -i.$$

Es muss nun nach §. 53, 2. in G eine Substitution χ geben, so dass

$$\chi(-1) = 0,\quad \chi(+1) = \infty$$

ist, und wenn man den constanten Factor wie bei der Tetraëdergruppe bestimmt [§. 56, (2)], so findet sich

(5) $$\chi(x) = i\,\frac{x+1}{x-1}.$$

Hieraus erhalten wir

$$\chi^2(x) = \frac{x+i}{x-i},\quad \chi^3(x) = x,$$

und die Relationen

(6) $$\Theta\chi = \chi^2\psi\Theta^3,\quad \Theta^2\chi = \chi\psi,\quad \Theta^3\chi = \chi^2\Theta$$
$$\psi\chi = \chi\psi\Theta^2,\quad \psi\chi^2 = \chi^2\Theta^2.$$

Diese Relationen in Verbindung mit (2) zeigen, dass die Substitutionen

(7) $$\chi^\lambda\psi^\mu\Theta^\nu,\quad \lambda = 0, 1, 2;\quad \mu = 0, 1;\quad \nu = 0, 1, 2, 3$$

in der That eine Gruppe bilden, weil man mit ihrer Hülfe jede Substitution der Form

$$\chi^\lambda\psi^\mu\Theta^\nu\chi,\quad \chi^\lambda\psi^\mu\Theta^\nu\psi,$$

und folglich durch Wiederholung auch jede Substitution

$$\chi^\lambda\psi^\mu\Theta^\nu\chi^{\lambda'}\psi^{\mu'}\Theta^{\nu'}$$

in die Form (7) bringen kann. Die Gruppe kann explicite in der Form

(8) $$i^\nu x,\ \frac{i^\nu}{x},\ i^\nu\frac{x - i^{\nu'}}{x + i^{\nu'}},\quad \nu, \nu' = 0, 1, 2, 3$$

dargestellt werden und ist vom 24sten Grade. Es ist die Octaëdergruppe.

Die Gruppe hat einen Normaltheiler 12ten Grades, den man in der Form $\chi^\lambda\psi^\mu\Theta^{2\nu}$ darstellen kann und der eine Tetraëdergruppe ist.

Die Darstellung wird in gewisser Beziehung einfacher, wenn man an Stelle von ψ ein neues Element

(9) $$\omega = \psi\Theta = \frac{-i}{x}$$

einführt, was ebenso wie ψ von der zweiten Ordnung ist. Dann kann die Gruppe dargestellt werden durch

$$\chi^\lambda\omega^\mu\Theta^\nu,$$

und an Stelle der Relationen (2) und (6) treten die folgenden:

$$\omega\chi = \chi^2\omega,\quad \omega\chi^2 = \chi\omega$$

(10) $$\Theta\chi = \chi^2\omega\Theta^2,\ \Theta^2\chi = \chi\omega\Theta^3,\ \Theta^3\chi = \chi^2\Theta,\ \Theta^2\chi^2 = \chi^2\omega\Theta$$
$$\Theta\omega = \omega\Theta^3,\quad \Theta^2\omega = \omega\Theta^2,\quad \Theta^3\omega = \omega\Theta.$$

Alle diese Relationen aber ergeben sich als Folgerungen aus den vieren:

(11) $$\omega\chi = \chi^2\omega,\quad \Theta\omega = \omega\Theta^3,\quad \Theta\chi = \chi^2\omega\Theta^2,\quad \Theta^2\chi = \chi\omega\Theta^3,$$

in Verbindung mit den die Grade ausdrückenden Formeln:

(12) $$\chi^3 = 1,\quad \omega^2 = 1,\quad \Theta^4 = 1.$$

Es folgt nämlich zunächst aus der zweiten der Relationen (11):

$$\Theta^2\omega = \Theta\omega\Theta^3 = \omega\Theta^2,\quad \Theta^3\omega = \Theta\omega\Theta^2 = \omega\Theta,$$

ferner aus der letzten (11):

$$\Theta^3\chi = \Theta\chi\omega\Theta^3 = \chi^2\omega\Theta^2\omega\Theta^3 = \chi^2\Theta,$$

und weiter:

$$\omega\chi^2 = \chi^2\omega\chi = \chi\omega,$$

$$\Theta^2\chi^2 = \chi\omega\Theta^3\chi = \chi\omega\chi^2\Theta = \chi^2\omega\Theta.$$

Wenn wir nun irgend drei Elemente χ, ω, Θ haben, die sich nach irgend einer Regel componiren lassen, wenn dabei χ vom dritten, ω vom zweiten, Θ vom vierten Grade ist, so folgt aus dem Bestehen der Relationen (11), dass die Elemente $\chi^\lambda\omega^\mu\Theta^\nu$ eine Gruppe 24sten Grades bilden, die mit der Octaëdergruppe isomorph ist. Dazu ist nur noch nachzuweisen, dass aus diesen Voraussetzungen folgt, dass die 24 Elemente $\chi^\lambda\omega^\mu\Theta^\nu$ alle von einander verschieden sind. Nehmen wir an, es sei

$$\chi^\lambda\omega^\mu\Theta^\nu = \chi^{\lambda'}\omega^{\mu'}\Theta^{\nu'},$$

so würde folgen:

$$\chi^{\lambda-\lambda'} = \omega^{\mu'}\Theta^{\nu'-\nu}\omega^{-\mu},$$

und nach (11):

$$\chi^{\lambda-\lambda'} = \omega^{\mu'-\mu}\Theta^{\pm(\nu-\nu')}.$$

Nun folgt aber aus (11), dass $\omega\Theta$, $\omega\Theta^2$, $\omega\Theta^3$ vom zweiten Grade sind, und da χ vom dritten Grade ist, so kann diese Beziehung nur stattfinden, wenn $\lambda-\lambda'$ durch 3, $\mu-\mu'$ durch 2 und $\nu-\nu'$ durch 4 theilbar, also $\chi^\lambda = \chi^{\lambda'}$, $\omega^\mu = \omega^{\mu'}$, $\Theta^\nu = \Theta^{\nu'}$ ist.

Nach der aus (10) folgenden Relation

$$\omega = \chi\Theta\chi\Theta^2$$

können wir ω aus χ und Θ zusammensetzen und daher χ und Θ als erzeugende Substitutionen der Gruppe ansehen.

Die noch fehlenden beiden Grundformen achten und zwölften Grades findet man sehr leicht, wenn man zunächst die Hesse'sche Covariante von f bildet.

Man erhält so die Grundform achten Grades:

$$W = x_1^8 + 14x_1^4x_2^4 + x_2^8, \tag{13}$$

und wenn man aus f und W die Functionaldeterminante bildet, die ja wieder eine Covariante von f ist (Bd. I, §. 59, 60), so ergiebt sich die Grundform zwölften Grades:

$$K = x_1^{12} - 33x_1^8x_2^4 - 33x_1^4x_2^8 + x_2^{12}. \tag{14}$$

Die Wurzeln von f entsprechen den sechs Octaëderecken oder den sechs Würfelflächen; die Wurzeln von W den acht Octaëderflächen oder Würfelecken, und die Wurzeln von K sowohl beim Octaëder als beim Würfel den 12 Kanten (vgl. §. 48).

Wenn man die Formen W, K so darstellt:

$$W = (x_1^4 + x_2^4)^2 + 12\, x_1^4 x_2^4, \quad K = (x_1^4 + x_2^4)^3 - 36\, x_1^4 x_2^4 (x_1^4 + x_2^4),$$

so lässt sich leicht die zwischen den drei Functionen f, W, K bestehende identische Relation ableiten:

$$(15) \qquad W^3 - K^2 = 108 f^4.$$

Die Octaëdergruppe enthält, wie man sieht, die Tetraëdergruppe und entsteht aus ihr durch Hinzunahme der einen Substitution $\Theta(x) = ix$. Die Grundformen des Octaëders sind also zugleich invariante Formen des Tetraëders, und in der That stimmen die Formen f des Tetraëders und Octaëders mit einander genau überein, und es ist $W = \Phi_1 \Phi_2$,

$$K = \tfrac{1}{2}(\Phi_1^3 + \Phi_2^3), \quad (§. 56).$$

Mit der Determinante 1 geschrieben, lauten die beiden erzeugenden Substitutionen der Octaëdergruppe so:

$$\Theta = \begin{pmatrix} \sqrt{i}, & 0 \\ 0, & \dfrac{1}{\sqrt{i}} \end{pmatrix}, \quad \chi = \begin{pmatrix} \dfrac{1}{\sqrt{2i}}, & \dfrac{1}{\sqrt{2i}} \\ \dfrac{1}{i\sqrt{2i}}, & \dfrac{-1}{i\sqrt{2i}} \end{pmatrix},$$

worin $\sqrt{2i} = 1 + i$ zu setzen ist.

Durch die Substitution Θ ändert nun die Form $f(x_1, x_2)$, wie die Formel (3) unmittelbar zeigt, ihr Vorzeichen. Durch Anwendung von χ werden die linearen Factoren von f folgendermaassen verändert:

$$\begin{array}{cccccc} x_1, & x_2, & x_1 + x_2, & x_1 - x_2, & x_1 + ix_2, & x_1 - ix_2 \\ \dfrac{x_1 + x_2}{\sqrt{2i}}, & \dfrac{x_1 - x_2}{i\sqrt{2i}}, & -i(x_1 + ix_2), & (x_1 - ix_2), & \dfrac{2x_1}{\sqrt{2i}}, & \dfrac{2x_2}{\sqrt{2i}}, \end{array}$$

und daraus geht hervor, dass $f(x_1, x_2)$ durch Anwendung der Substitution χ ungeändert bleibt, und dadurch sind die Aenderungen der Form f durch alle anderen Octaëdersubstitutionen zugleich mit bestimmt.

Die Hesse'sche Covariante W von f bleibt ungeändert, wenn f in $-f$ verwandelt wird, und folglich bleibt W bei den

Octaëdersubstitutionen absolut ungeändert, während K wieder die gleichen Vorzeichenänderungen wie f erleidet.

§. 58.

Die Ikosaëdergruppe.

Da wir bei der Ikosaëdergruppe nur ein System conjugirter fünfzähliger Pole haben, so können wir (§. 53, 1.) in dieser Gruppe die beiden Substitutionen

$$(1) \qquad \Theta(x) = \varepsilon x, \quad \psi(x) = \frac{-1}{x}$$

annehmen, worin ε eine primitive fünfte Einheitswurzel bedeutet. Wir nehmen hier, was freisteht, die Substitutionen ψ in der Form $-1 : x$ an, weil dadurch die Formeln einfacher werden. Die zu dem Systeme der fünfzähligen Pole gehörige Grundform 12ten Grades muss, da sie die Substitutionen (1) gestattet, von der Form sein:

$$(2) \qquad f(x_1, x_2) = x_1 x_2 (x_1^{10} + m x_1^5 x_2^5 - x_2^{10}),$$

und es handelt sich noch um die Bestimmung des constanten Factors m. Die beiden anderen Grundformen sind vom 20sten und 30sten Grade. Wir können nun m nach dem Satze §. 54, 4. bestimmen, wenn wir eine Covariante von $f(x)$ bilden können, deren Grad niedriger als 60 ist, und die sich nicht als ein Product aus Potenzen von drei Functionen 12ten, 20sten, 30sten Grades darstellen lässt, die nach dem erwähnten Satze identisch Null sein muss.

Nun lässt sich leicht eine Covariante 16ten Grades von der Form f bilden, wenn wir nach Bd. I, §. 60 die vierte Polare der Form $f(x_1, x_2)$ nehmen:

$$12 \,.\, 11 \,.\, 10 \,.\, 9 \; P_4(x, \xi) =$$
$$u_0 \xi_1^4 + u_1 \xi_1^3 \xi_2 + u_2 \xi_1^2 \xi_2^2 + u_3 \xi_1 \xi_2^3 + u_4 \xi_2^4,$$

worin

$$u_0 = \frac{\partial^4 f}{\partial x_1^4}, \quad u_1 = 4 \frac{\partial^4 f}{\partial x_1^3 \partial x_2}, \quad u_2 = 6 \frac{\partial^4 f}{\partial x_1^2 \partial x_2^2},$$
$$u_3 = 4 \frac{\partial^4 f}{\partial x_1 \partial x_2^3}, \quad u_4 = \frac{\partial^4 f}{\partial x_2^4}.$$

Daraus erhalten wir eine Covariante 16ten Grades von f als

erste Invariante der in Bezug auf die Variablen ξ_1, ξ_2 biquadratischen Form, nämlich (Bd. I, §. 64):

(3) $$u_2^2 - 3 u_1 u_3 + 12 u_0 u_4.$$

Da aber eine Form 16ten Grades sich nicht als Product von Formen 12ten, 20sten und 30sten Grades darstellen lassen kann, so muss diese Covariante identisch verschwinden. Nun ist hier

$$\begin{aligned}
u_0 &= 11.10.9.8\, x_1^7 x_2 + 6.5.4.3\, m\, x_1^2 x_2^6, \\
u_1 &= 4.11.10.9\, x_1^8 + 4.6.5.4.6\, m\, x_1^3 x_2^5, \\
u_2 &= 6^3.5^2\, m\, x_1^4 x_2^4, \\
u_3 &= -\,4.11.10.9\, x_2^8 + 4.6.5.4.6\, m\, x_2^3 x_1^5, \\
u_4 &= -\,11.10.9.8\, x_2^7 x_1 + 6.5.4.3\, m\, x_2^2 x_1^6,
\end{aligned}$$

und wenn wir daraus die Covariante (3) bilden und den Coëfficienten von $x_1^8 x_2^8$ gleich 0 setzen, so ergiebt sich $m = \pm 11$. Beide Zahlen sind hier zulässig. Die eine Annahme wird auf die andere zurückgeführt durch die Vertauschung von x_1 mit $-x_1$, also durch eine Transformation der Gruppe. Wir setzen demnach:

(4) $$f(x_1, x_2) = x_1 x_2 (x_1^{10} + 11\, x_1^5 x_2^5 - x_2^{10}).$$

Die zehn noch fehlenden fünfzähligen Pole erhält man also durch Auflösung der Gleichung

$$x^{10} + 11\, x^5 - 1 = 0,$$

aus der man

$$x^5 = \frac{-11 \pm 5\sqrt{5}}{2} = \left(\frac{-1 \pm \sqrt{5}}{2}\right)^5$$

findet. Setzen wir demnach

(5) $$\begin{aligned}
\omega &= \varepsilon + \varepsilon^4 = 2\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{2}, \\
\omega' &= \varepsilon^2 + \varepsilon^3 = 2\cos\frac{4\pi}{5} = \frac{-1-\sqrt{5}}{2}
\end{aligned}$$

so dass

(6) $$\omega^2 + \omega = 1, \quad \omega + \omega' = -1, \quad \omega\omega' = -1$$

ist, so sind die fünfzähligen Pole ausser 0 und ∞:

(7) $$\xi = \varepsilon^\lambda \omega, \quad \varepsilon^\lambda \omega' = \frac{-\varepsilon^\lambda}{\omega}, \quad \lambda = 0, 1, 2, 3, 4.$$

Nun wenden wir den Satz §. 53, 2. an, nach dem, wenn a, a' zwei Pole einer Substitution Θ sind, und b ein zu a conjugirter Pol ist, eine Substitution χ in der Gruppe existiren muss, so

dass $b = \chi(a)$, $b' = \chi(a')$ die beiden Pole der Substitution $\chi^{-1}\Theta\chi$ sind. Darin können wir ∞ und 0 für a und a' nehmen. und ω für b. Dann wird b' ein noch näher zu bestimmender Pol ξ aus der Reihe (7), und für χ erhalten wir die Form

$$\chi(x) = \frac{\alpha x + \beta}{\gamma x + \delta} = \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix},$$

worin

(8) $$\omega = \frac{\alpha}{\gamma}, \quad \xi = \frac{\beta}{\delta}$$

zu setzen ist.

Nun können wir für Θ jede der Substitutionen $\varepsilon^h x$ nehmen, wenn nur h nicht durch 5 theilbar ist, und erhalten so die Substitution

$$\chi^{-1}\Theta\chi = \begin{pmatrix}\delta, & -\beta \\ -\gamma, & \alpha\end{pmatrix}\begin{pmatrix}\varepsilon^h, & 0 \\ 0, & 1\end{pmatrix}\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$$
$$= \begin{pmatrix}\varepsilon^h \alpha\delta - \beta\gamma, & (\varepsilon^h - 1)\beta\delta \\ -(\varepsilon^h - 1)\alpha\gamma, & \alpha\delta - \varepsilon^h\beta\gamma\end{pmatrix},$$

deren Pole ω und ξ sein müssen. Nach §. 51, (6) müssen also ω und ξ die Wurzeln der quadratischen Gleichung

$$\alpha\gamma x^2 + (\alpha\delta + \beta\gamma)x + \beta\delta = 0$$

sein, woraus

$$\frac{\beta\delta}{\alpha\gamma} = \omega\xi, \quad \frac{\delta}{\gamma} + \frac{\beta}{\alpha} = -\omega - \xi$$

folgt. Aus der zweiten dieser Gleichungen ergiebt sich mittelst (8):

$$(\alpha + \delta)(\alpha\delta + \beta\gamma) = 0,$$

und da $\alpha\delta + \beta\gamma$ nicht verschwinden kann, weil sonst $\omega + \xi = 0$ sein müsste, was nach (7) nicht möglich ist, so ist $\alpha + \delta = 0$. Danach erhalten wir für χ, wenn wir der Einfachheit halber $\gamma = 1$ annehmen:

(9) $$\chi = \begin{pmatrix}\omega, & \beta \\ 1, & -\omega\end{pmatrix}.$$

Hierin ist β, was nach (8) den Werth $-\omega\xi$ hat, noch zu bestimmen.

Wenn wir die Substitution χ als bekannt annehmen, so können wir die ganze Ikosaëdergruppe bilden.

Man hat nämlich, wenn man r und s die Zahlen 0, 1, 2, 3, 4 durchlaufen lässt, in dieser Gruppe die Substitutionen

(10) $$\Theta^r, \quad \psi\Theta^r, \quad \Theta^r\chi\Theta^s, \quad \Theta^r\chi\psi\Theta^s,$$

deren Zahl gerade 60 beträgt. Dass sie alle von einander verschieden sind, sieht man, wenn man sie in der Form darstellt:

(11) $$\Theta^r = \begin{pmatrix} \varepsilon^r, & 0 \\ 0, & 1 \end{pmatrix},$$

(12) $$\psi\,\Theta^r = \begin{pmatrix} 0, & 1 \\ -\varepsilon^r, & 0 \end{pmatrix},$$

(13) $$\Theta^r \chi\, \Theta^s = \begin{pmatrix} \varepsilon^r \omega, & \varepsilon^{r-s}\beta \\ 1, & -\varepsilon^{-s}\omega \end{pmatrix},$$

(14) $$\Theta^r \chi\, \psi\, \Theta^s = \begin{pmatrix} -\varepsilon^{r+s}\beta, & \varepsilon^r \omega \\ \varepsilon^s \omega, & 1 \end{pmatrix}$$

$$= \begin{pmatrix} -\varepsilon^r \beta\, \omega^{-1}, & \varepsilon^{r-s} \\ 1, & \varepsilon^{-s}\omega^{-1} \end{pmatrix},$$

von denen, da $-\omega^2$ keine Potenz von ε ist, ersichtlich keine zwei einander gleich sind.

Die Ikosaëdergruppe hat, wie wir gesehen haben, 12 fünfzählige Pole. Je zwei dieser Pole sind die Pole von vier Substitutionen 5ten Grades, die mit der Identität zusammen einen fünfgliedrigen Cyklus bilden. Folglich giebt es in der Gruppe 24 Elemente 5ten Grades. Ebenso giebt es 20 dreizählige Pole, die zu 20 Substitutionen dritter Ordnung führen, und 30 zweizählige Pole, die zu zweien die Pole von je einer Substitution zweiter Ordnung sind, so dass es 15 Substitutionen zweiter Ordnung giebt. Dies giebt mit der Identität zusammen

$$24 + 20 + 15 + 1 = 60.$$

Die Bestimmung von β in der Substitution χ ergiebt sich nun durch Betrachtung der Grade von (13) und (14). Wir bilden dazu zunächst für eine beliebige lineare Substitution $S = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ die zweite und dritte Wiederholung:

$$S^2 = \begin{pmatrix} a^2 + bc, & b(a+d) \\ c(a+d), & bc + d^2 \end{pmatrix}$$

$$S^3 = \begin{pmatrix} a^3 + 2abc + bcd, & b(a^2 + bc + ad + d^2) \\ c(a^2 + bc + ad + d^2), & d^3 + abc + 2bcd \end{pmatrix},$$

und wenn wir von dem Falle absehen, dass b oder c verschwindet, der hier nicht in Betracht kommt, so erhalten wir die nothwendige und hinreichende Bedingung:

für eine Substitution zweiter Ordnung

(15) $$a + d = 0,$$

und für eine Substitution dritter Ordnung

(16) $$a^2 + bc + ad + d^2 = 0.$$

Nun sind die Substitutionen (11), abgesehen von der darunter enthaltenen identischen, von der fünften Ordnung. Die fünf Substitutionen (12) sind von der zweiten Ordnung. Von den Substitutionen (13) sind nach (15) die fünf in der Form $\Theta^r \chi \Theta^{-r}$ enthaltenen (und nur diese) von der zweiten Ordnung, und folglich müssen noch fünf von den Substitutionen (14) von der zweiten Ordnung sein. Dies ist aber nach (15) nur möglich, wenn β eine Potenz von ε ist.

Die Substitutionen dritter Ordnung müssen sich nun auf die Formen (13) und (14) vertheilen. Für diese ergeben sich nach (16) die Bedingungen:

dass (13) von der dritten Ordnung sei

(17) $$\omega^2 (\varepsilon^{r+s} + \varepsilon^{-(r+s)} - 1) = -\beta,$$

und dass (14) von der dritten Ordnung sei

(18) $$\omega^2 = \beta - \varepsilon^{-(r+s)} - \beta^2 \varepsilon^{r+s}.$$

Soll aber auch nur eine der beiden Bedingungen (17) oder (18) befriedigt werden können, so muss

$$\beta = 1$$

sein. Denn ω^2 ist reell und die ganze linke Seite von (17) ist also gleichfalls reell; folglich muss β reell, und da es eine Potenz von ε ist, gleich 1 sein.

Soll aber (18) befriedigt werden, so darf sich die linke Seite nicht ändern, wenn man zu den conjugirt imaginären Grössen übergeht; d. h. es muss

$$\beta - \varepsilon^{-(r+s)} - \beta^2 \varepsilon^{r+s} = \beta^{-1} - \varepsilon^{r+s} - \beta^{-2} \varepsilon^{-(r+s)}$$

oder

$$(\beta - \beta^{-1})(1 - \beta^{-1} \varepsilon^{-(r+s)} - \beta \varepsilon^{r+s}) = 0$$

sein, und dies ist, weil β eine Potenz von ε ist, nur möglich, wenn $\beta = \beta^{-1}$, also $\beta = 1$ ist.

Hiernach sind fünf von den Substitutionen (14) von der zweiten Ordnung, nämlich $\Theta^r \chi \psi \Theta^{-r}$, und es ergiebt sich, dass (13) von der dritten Ordnung ist, wenn

$$\omega^2 (\varepsilon^{r+s} + \varepsilon^{-(r+s)} - 1) = -1,$$

oder, wenn man mit ω'^2 multiplicirt, nach (5) und (6)

$$\varepsilon^{r+s} + \varepsilon^{-(r+s)} - 1 = -\varepsilon - \varepsilon^{-1} - 2$$
$$\varepsilon + \varepsilon^{-1} + \varepsilon^{r+s} + \varepsilon^{-(r+s)} + 1 = 0,$$

eine Bedingung, die dann und nur dann erfüllt ist, wenn $r + s \equiv \pm 2 \pmod 5$ ist.

Wenn (14) von der dritten Ordnung sein soll, so muss nach (18) und (5)

$$\varepsilon^2 + \varepsilon^{-2} + 2 = 1 - \varepsilon^{-(r+s)} - \varepsilon^{r+s}$$
$$\varepsilon^2 + \varepsilon^{-2} + \varepsilon^{r+s} + \varepsilon^{-(r+s)} + 1 = 0$$

sein, und diese Bedingung ist dann und nur dann befriedigt, wenn $r + s \equiv \pm 1 \pmod 5$ ist.

Hiernach erhalten wir, wie es sein muss, in (13) und (14) gerade 10 Substitutionen zweiter und 20 Substitutionen dritter Ordnung, und die anderen Fälle bleiben also für die fünfte Ordnung übrig.

Fassen wir das Resultat dieser Betrachtung zusammen, so haben wir:

Die Substitution χ muss den Ausdruck haben:

(19) $$\chi = \begin{pmatrix} \omega, & 1 \\ 1, & -\omega \end{pmatrix},$$

und unter den 60 Substitutionen (10):

(20) $$\Theta^r,\ \psi\Theta^r,\ \Theta^r\chi\Theta^s,\ \Theta^r\chi\psi\Theta^s$$

kommen ausser der Identität vor:

15 Substitutionen 2ten Grades:

$$\psi\Theta^r,\ \Theta^r\chi\Theta^{-r},\ \Theta^r\chi\psi\Theta^{-r},\ r = 0, 1, 2, 3, 4,$$

(21) 20 Substitutionen 3ten Grades:

$$\Theta^r\chi\Theta^s,\quad r + s \equiv \pm 2 \pmod 5$$
$$\Theta^r\chi\psi\Theta^s,\quad r + s \equiv \pm 1 \pmod 5,$$

24 Substitutionen 5ten Grades:

$$\Theta^r,\ \Theta^r\chi\Theta^s,\quad r + s \equiv \pm 1 \pmod 5$$
$$\Theta^r\chi\psi\Theta^s,\quad r + s \equiv \pm 2 \pmod 5.$$

In expliciter Form erhält man für die Substitutionen (20) den Ausdruck:

(22) $$\begin{pmatrix} \varepsilon^r, & 0 \\ 0, & 1 \end{pmatrix},\ \begin{pmatrix} 0, & \varepsilon^r \\ -1, & 0 \end{pmatrix},\ \begin{pmatrix} \varepsilon^r\omega, & \varepsilon^{r-s} \\ 1, & -\varepsilon^{-s}\omega \end{pmatrix},\ \begin{pmatrix} -\varepsilon^{r+s}, & \varepsilon^r\omega \\ \varepsilon^s\omega, & 1 \end{pmatrix}$$

oder

$$\varepsilon^r x,\ \frac{-\varepsilon^r}{x},\ \frac{\varepsilon^r\omega x + \varepsilon^{r-s}}{x - \varepsilon^{-s}\omega},\ \frac{-\varepsilon^{r+s}x + \varepsilon^r\omega}{\varepsilon^s\omega x + 1}.$$

Um also endlich die Existenz der Ikosaëdergruppe festzustellen, ist noch nachzuweisen, dass die Gesammtheit der Substitutionen (20) eine Gruppe bildet. Dies folgt aber aus den nun abzuleitenden Compositionsgesetzen.

Zunächst ergiebt sich sehr einfach aus der Bedeutung von Θ, ψ, χ:

$$\Theta = \begin{pmatrix} \varepsilon, & 0 \\ 0, & 1 \end{pmatrix}, \quad \psi = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad \chi = \begin{pmatrix} \omega, & 1 \\ 1, & -\omega \end{pmatrix}$$

(23) $$\psi\Theta = \Theta^{-1}\psi, \quad \chi\psi = \psi\chi.$$

Ferner erhält man für jeden beliebigen Exponenten λ:

$$\chi\Theta^{\lambda}\chi = \begin{pmatrix} \varepsilon^{\lambda}\omega^2 + 1, & (\varepsilon^{\lambda} - 1)\omega \\ (\varepsilon^{\lambda} - 1)\omega, & \varepsilon^{\lambda} + \omega^2 \end{pmatrix},$$

oder, indem man nach (5) und (6)

(24) $$\omega = \varepsilon + \varepsilon^{-1}, \quad \omega' = \varepsilon^2 + \varepsilon^{-2}, \quad \omega\omega' = -1$$

setzt:

$$\chi\Theta^{\lambda}\chi = \begin{pmatrix} \varepsilon^{\lambda}\omega - \omega', & \varepsilon^{\lambda} - 1 \\ \varepsilon^{\lambda} - 1, & -\varepsilon^{\lambda}\omega' + \omega \end{pmatrix}.$$

Setzen wir darin zunächst $\lambda = 1$, so folgt nach (24), (13), (14):

$$\chi\Theta\chi = \begin{pmatrix} 1 - \varepsilon^3, & \varepsilon - 1 \\ \varepsilon - 1, & \varepsilon - \varepsilon^3 \end{pmatrix} = \begin{pmatrix} \varepsilon^3(\varepsilon + 1), & 1 \\ 1, & -\varepsilon(\varepsilon + 1) \end{pmatrix}$$
$$= \begin{pmatrix} \varepsilon\omega', & 1 \\ 1, & -\varepsilon^{-1}\omega' \end{pmatrix} = \begin{pmatrix} -\varepsilon^2, & \varepsilon\omega \\ \varepsilon\omega, & 1 \end{pmatrix} = \Theta\chi\psi\Theta,$$

woraus, wenn man beiderseits zur entgegengesetzten Substitution übergeht,

$$\chi\Theta^{-1}\chi = \Theta^{-1}\chi\psi\Theta^{-1}$$

folgt. Setzt man andererseits $\lambda = 2$, so folgt:

$$\chi\Theta^2\chi = \begin{pmatrix} \varepsilon - \varepsilon^2, & \varepsilon^2 - 1 \\ \varepsilon^2 - 1, & \varepsilon - 1 \end{pmatrix} = \begin{pmatrix} \varepsilon^2(\varepsilon^2 + 1), & 1 \\ 1, & -\varepsilon(\varepsilon^2 + 1) \end{pmatrix}$$
$$= \begin{pmatrix} \varepsilon^3\omega, & 1 \\ 1, & -\varepsilon^2\omega \end{pmatrix} = \Theta^{-2}\chi\Theta^{-2},$$

worin wieder Θ durch Θ^{-1} ersetzt werden kann. Man hat daher die Compositionsformeln:

(25) $$\chi\Theta^{\pm 1}\chi = \Theta^{\pm 1}\chi\psi\Theta^{\pm 1}, \quad \chi\Theta^{\pm 2}\chi = \Theta^{\mp 2}\chi\Theta^{\mp 2}.$$

Durch Anwendung der Formeln (23) und (25) kann man nun je zwei der Substitutionen (20) componiren und gelangt immer wieder auf eine Substitution von der Form (20), wodurch

die Gruppennatur nachgewiesen und die Ikosaëdergruppe gebildet ist.

Aus der ersten Formel (25) ergiebt sich noch

$$\psi = \chi \Theta^{\mp 1} \chi \Theta^{\pm 1} \chi \Theta^{\mp 1},$$

woraus man schliesst, dass ψ aus χ und Θ abgeleitet werden kann, dass also χ und Θ allein schon als erzeugende Substitutionen der Ikosaëdergruppe betrachtet werden können.

Wollen wir die Substitution χ mit der Determinante 1 darstellen, so beachten wir die Relation

$$-\omega^2 - 1 = \omega - 2 = (\varepsilon^2 - \varepsilon^{-2})^2,$$

und erhalten, wenn wir noch $\varepsilon + \varepsilon^{-1}$ für ω einsetzen:

$$(26) \qquad \chi = \begin{pmatrix} \frac{1}{\varepsilon - \varepsilon^{-1}}, & \frac{1}{\varepsilon^2 - \varepsilon^{-2}} \\ \frac{1}{\varepsilon^2 - \varepsilon^{-2}}, & \frac{-1}{\varepsilon - \varepsilon^{-1}} \end{pmatrix}.$$

§. 59.

Die Theiler der Ikosaëdergruppe.

Die Theiler der Ikosaëdergruppe müssen unter den niedrigeren Polyëdergruppen gesucht werden. Darunter finden sich zunächst die cyklischen Gruppen C_n, deren jede aus der Periode einer der Ikosaëdersubstitutionen besteht. Die Abzählung der Anzahl dieser Gruppen ergiebt sich sofort aus der Zusammenstellung der Substitutionen nach ihren Graden, wie wir sie im vorigen Paragraphen gegeben haben; nämlich:

15 Gruppen C_2,
10 „ C_3,
6 „ C_5.

Es sind ferner in der Ikosaëdergruppe Diëdergruppen D_2, D_3, D_5 enthalten, als deren Repräsentanten wir folgende aufstellen:

$$\begin{aligned} D_2 &: 1, \psi, \chi, \psi\chi, \\ D_3 &: 1, \chi\Theta^2, \Theta^{-2}\chi, \psi\chi, \psi\Theta^2, \Theta^{-2}\psi\chi\Theta^2, \\ D_5 &: \Theta^r, \psi\Theta^r, \qquad r = 0, 1, 2, 3, 4, 5. \end{aligned}$$

Die Anzahl der Diëdergruppen erhalten wir daraus, dass die Diëdergruppe durch die in ihr enthaltene cyklische Gruppe vollständig bestimmt ist (§. 55). Bei der Vierergruppe ist aber noch zu beachten, dass man dieselbe Gruppe erhält, wenn man von ψ, von χ oder von $\psi\chi$ ausgeht, und dass also die direct erhaltene Zahl durch 3 zu dividiren ist. Die Anzahl der D_2 ist also 5, die der D_3 ist 10 und die der D_5 ist 6.

Von besonderer Wichtigkeit sind aber die in der Ikosaëdergruppe enthaltenen Tetraëdergruppen. Wir wollen eine von ihnen, die wir mit Q bezeichnen, bestimmen.

Die Tetraëdergruppe muss (nach §. 56) eine Vierergruppe D_2 enthalten. Wir gehen von einer solchen Gruppe D_2 aus und wählen dazu

$$1, \ \psi, \ \chi, \ \psi\chi.$$

Es muss nun weiter in Q eine Substitution dritter Ordnung vorkommen. Diese können wir in einer der beiden Formen $\Theta^r\chi\Theta^s$ oder $\Theta^r\chi\psi\Theta^s$ annehmen. Da beide Annahmen zu demselben Resultate führen, wählen wir als Substitution dritter Ordnung

$$\varphi = \Theta^r\chi\Theta^s, \quad r + s \equiv \pm 2 \pmod 5 \quad [\text{§. 58, (21)}].$$

Von den Zahlen r, s kann aber keine $\equiv 0$ sein, weil sonst entweder $\chi\varphi$ oder $\varphi\chi$ eine Potenz von Θ, also vom 5ten Grade wäre, während doch in Q kein Element 5ten Grades vorkommen kann.

Wir bilden ferner nach §. 58, (23), (25):

$$\chi\varphi = \Theta^r\chi\psi\Theta^{r+s}, \quad r \equiv \pm 1$$
$$\chi\varphi = \Theta^{-r}\chi\Theta^{-r+s}, \quad r \equiv \pm 2,$$

wodurch aus dem oben angeführten Grunde im ersten Falle $r \equiv -s$, im zweiten $r \equiv s$ ausgeschlossen ist, und im ersten Falle $2r + s \equiv \pm 1$, im zweiten $-2r + s \equiv \pm 2$ gefordert wird. Danach bleiben die vier möglichen Fälle

$$r \equiv \pm 1, \quad s \equiv \pm 2, \quad r \equiv \pm 2, \quad s \equiv \pm 1 \pmod 5)$$

übrig.

Wenn von den so bestimmten vier Substitutionen dritter Ordnung eine in Q vorkommt, so kommen auch die drei anderen vor. Denn setzen wir

(1) $$\varphi = \Theta\chi\Theta^2,$$

so ergiebt sich nach §. 58, (23), (25):

(2) $$\varphi^{-1} = \Theta^{-2}\chi\Theta^{-1}, \quad \varphi\chi = \Theta^{-1}\chi\Theta^{-2}, \quad \chi\varphi^{-1} = \Theta^2\chi\Theta.$$

Bildet man ausserdem noch $\varphi\psi$, $\varphi^{-1}\psi$, $\varphi\chi\psi$, $\chi\varphi^{-1}\psi$, so folgt:

$$\varphi\psi = \Theta\chi\psi\Theta^{-2},\quad \varphi^{-1}\psi = \Theta^{-2}\chi\psi\Theta,\quad \varphi\chi\psi = \Theta^{-1}\chi\psi\Theta^{2},$$
$$\chi\varphi^{-1}\psi = \Theta^{2}\chi\psi\Theta^{-1},$$

woraus man sieht, dass man zu keinem anderen Resultate kommen würde, wenn man die Substitution dritter Ordnung, von der man ausgeht, in der zweiten Form $\Theta^r\chi\psi\Theta^s$ annehmen wollte. Die ganze Gruppe Q ist also durch die angenommene Vierergruppe D_2 völlig bestimmt, und man erhält sie in der Form

$$(3)\qquad \begin{array}{ll} 1 & \psi \\ \varphi = \Theta\chi\Theta^{2}, & \varphi\psi = \Theta\chi\psi\Theta^{-2}, \\ \varphi^{-1} = \Theta^{-2}\chi\Theta^{-1}, & \varphi^{-1}\psi = \Theta^{-2}\chi\psi\Theta, \\ \chi & \chi\psi \\ \varphi\chi = \Theta^{-1}\chi\Theta^{-2}, & \varphi\chi\psi = \Theta^{-1}\chi\psi\Theta^{2}, \\ \varphi^{-1}\chi = \Theta^{2}\chi\psi\Theta^{-1}, & \varphi^{-1}\chi\psi = \Theta^{2}\chi\Theta. \end{array}$$

Man kann diese Gruppe aus den Substitutionen φ, ψ, χ als den Erzeugenden ableiten und sie in die Form setzen:

$$(4)\qquad Q = \varphi^r\chi^s\psi^t, \quad \begin{array}{l} r = 0, 1, 2, \\ s = 0, 1; \quad t = 0, 1. \end{array}$$

Dass dadurch wirklich eine Tetraëdergruppe dargestellt ist, ergiebt sich aus den Zusammensetzungen, die man mittelst §. 58, (23), (25) leicht aus (1) findet:

$$(5)\qquad \begin{array}{c} \psi\varphi = \varphi\chi\psi,\quad \chi\varphi = \varphi\psi, \\ \psi\varphi^{2} = \chi\varphi^{2}\psi,\quad \chi\varphi^{2} = \varphi^{2}\chi\psi,\quad \psi\chi = \chi\psi. \end{array}$$

Da in der Tetraëdergruppe fünf Vierergruppen D_2 enthalten sind, so hat die Ikosaëdergruppe fünf Tetraëdergruppen zu Theilern. Diese können wir aus Q durch Transformation mittelst der Potenzen von Θ ableiten und erhalten sie in der Form

$$\Theta^{-r}Q\Theta^{r}\qquad r = 0, 1, 2, 3, 4.$$

Diese Gruppen haben, ausser der Identität, keine Substitution mit einander gemein. Denn die beiden Gruppen Q und $\Theta^{-1}Q\Theta$ haben ausser der Identität nur die beiden Elemente

$$\Theta^{-2}\chi\Theta^{-1},\quad \Theta\chi\Theta^{2}$$

mit einander gemein, und von diesen kommt keines in $\Theta Q\Theta^{-1}$ vor.

Daraus ergiebt sich nun nach dem Satze 2. in §. 28, dass die Ikosaëdergruppe isomorph ist mit einer Permutationsgruppe

60sten Grades von fünf Ziffern. Diese Permutationsgruppe ergiebt sich, wenn wir mit den Nebengruppen

$$Q,\ Q\Theta,\ Q\Theta^2,\ Q\Theta^3,\ Q\Theta^4$$

die sämmtlichen Elemente σ der Ikosaëdergruppe verbinden, also

$$Q\sigma,\ Q\Theta\sigma,\ Q\Theta^2\sigma,\ Q\Theta^3\sigma,\ Q\Theta^4\sigma$$

bilden, und die dadurch bewirkte Permutation dieser Nebengruppen untersuchen. Für die erzeugenden Substitutionen der Ikosaëdergruppe $\sigma = \Theta, \psi, \chi$ erhalten wir so die Permutationen

$$(1,\ \Theta,\ \Theta^2,\ \Theta^3,\ \Theta^4) \qquad \sigma = \Theta$$

$$\begin{pmatrix} Q, & Q\Theta, & Q\Theta^2, & Q\Theta^3, & Q\Theta^4 \\ Q, & Q\Theta^4, & Q\Theta^3, & Q\Theta^2, & Q\Theta \end{pmatrix} \qquad \sigma = \psi$$

$$\begin{pmatrix} Q, & Q\Theta, & Q\Theta^2, & Q\Theta^3, & Q\Theta^4 \\ Q, & Q\Theta^3, & Q\Theta^4, & Q\Theta, & Q\Theta^2 \end{pmatrix} \qquad \sigma = \chi.$$

Letzteres findet man aus den Formeln (1) und (2), wonach

$$\Theta\chi = \varphi\Theta^3,\quad \Theta^2\chi = \chi\varphi^2\Theta^4,\quad \Theta^3\chi = \varphi^2\Theta,\quad \Theta^4\chi = \varphi\chi\Theta^2.$$

Man sieht, dass diese Permutationen alle zur ersten Art gehören, und dass also die Permutationsgruppe, um die es sich handelt, keine andere als die alternirende Gruppe von fünf Ziffern (Bd. I, §. 177) sein kann. Daraus ergiebt sich auch, dass die Ikosaëdergruppe einfach ist, und folglich mit der Gruppe übereinstimmt, die wir schon in §. 34 vorläufig als Ikosaëdergruppe bezeichnet haben.

§. 60.

Die Grundformen der Ikosaëdergruppe.

Wir haben oben die eine der drei Grundformen der Ikosaëdergruppe f gefunden:

$$(1) \qquad f = x_1 x_2 (x_1^{10} + 11 x_1^5 x_2^5 - x_2^{10}).$$

Es fehlen uns also noch zwei dieser Formen, eine vom 20sten und eine vom 30sten Grade.

Die Grundform 20sten Grades ergiebt sich als die Hesse'sche Covariante von f. Wir setzen sie

$$(2) \qquad H = \frac{1}{121}\,[f''(x_1, x_1)\, f''(x_2, x_2) - f''(x_1, x_2)^2],$$

und finden durch einfache Rechnung:

$$(3) \qquad H = -(x_1^{20} + x_2^{20}) + 228\,(x_1^{15} x_2^5 - x_2^{15} x_1^5) - 494\, x_1^{10} x_2^{10}.$$

Die Grundform 30sten Grades können wir als die Functionaldeterminante von H und f definiren. Setzen wir

$$(4) \qquad T = \frac{1}{20}\,[f'(x_1)\,H'(x_2) - f'(x_2)\,H'(x_1)],$$

so findet sich

$$(5) \qquad \begin{aligned} T = (x_1^{30} + x_2^{30}) &+ 522\,(x_1^{25} x_2^5 - x_1^5 x_2^{25}) \\ &- 10005\,(x_1^{20} x_2^{10} + x_2^{20} x_1^{10}). \end{aligned}$$

Auch zwischen diesen drei Formen besteht eine identische Relation. Um sie zu finden, setzen wir

$$\lambda = x_1^{10} - x_2^{10}, \quad \mu = x_1^5 x_2^5,$$

und erhalten, wenn wir bei T den Factor $x_1^{10} + x_2^{10}$ herausnehmen und dann T^2 bilden:

$$\begin{aligned} f^5 &= \mu\,(\lambda + 11\,\mu)^5, \\ H &= -\lambda^2 + 228\,\lambda\mu - 496\,\mu^2, \\ T^2 &= (\lambda^2 + 4\,\mu^2)\,(\lambda^2 + 522\,\lambda\mu - 10004\,\mu^2)^2. \end{aligned}$$

Daraus erhält man durch die numerische Berechnung

$$(6) \qquad T^2 + H^3 = 1728\, f^5,$$

was die gesuchte Relation ist.

Da die Ikosaëdergruppe, wie wir gesehen haben, einfach ist, so kann sie nach §. 40 keine relativen Invarianten haben. Daraus ergiebt sich, dass die Ikosaëderformen f, H, T absolut ungeändert bleiben, wenn man sie den mit der Determinante 1 dargestellten binären Ikosaëdersubstitutionen unterwirft. Dasselbe lässt sich aber auch, ohne jene allgemeinen Sätze zu benutzen, in folgender Weise direct nachweisen.

Die Relation (6) lässt sich in der Form darstellen:

$$(7) \qquad \frac{T^2}{f^5} + \frac{H^3}{f^5} = 1728,$$

und die beiden Quotienten $T^2 : f^5$, $H^3 : f^5$ können wir als Functionen der einen Veränderlichen $x = x_1 : x_2$ auffassen. Wenden wir auf diese Variable eine Substitution der Ikosaëdergruppe an, so ändern sich diese beiden Quotienten nur um constante Factoren, d. h. wenn wir

$$(8) \qquad \frac{T^2}{f^5} = \Phi(x), \quad \frac{H^3}{f^5} = \Psi(x), \quad y = \frac{\alpha x + \beta}{\gamma x + \delta}$$

setzen und mit h, k zwei Constanten bezeichnen, so ist

$$\Phi(y) = h\Phi(x), \quad \Psi(y) = k\Psi(x),$$

vorausgesetzt, dass $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ eine der Ikosaëdersubstitutionen ist. Da nun aber y sowohl als x eine unabhängige Variable ist, so besteht nach (7) die Identität

$$\Phi(x) + \Psi(x) = h\Phi(x) + k\Psi(x) = 1728,$$

und da Φ und Ψ nicht in constantem Verhältnisse stehen, so muss $h = k = 1$ sein, d. h. die Quotienten Φ und Ψ bleiben bei den Ikosaëdersubstitutionen absolut ungeändert.

Daraus ergiebt sich weiter, dass f, H, T bei den homogenen Ikosaëdersubstitutionen mit der Determinante 1 absolut ungeändert bleiben.

Denn wenn f durch eine solche Substitution in cf übergeht, so gehen H und T in $c^2 H$ und $c^3 T$ über [nach (2) und (4)], und die Quotienten Φ und Ψ in $c\Phi$ und $c\Psi$. Da andererseits Φ und Ψ ungeändert bleiben, so ist $c = 1$.

Setzen wir $\Psi(x) = z$, so wird $\Phi(x) = 1728 - z$, und wir erhalten aus (8) die beiden Gleichungen:

$$H^3 - zf^5 = 0, \tag{9}$$

$$T^2 - (1728 - z)f^5 = 0, \tag{10}$$

von denen wegen der Identität (6) die eine aus der anderen folgt, so dass es eigentlich nur zwei verschiedene Formen für eine und dieselbe Gleichung sind. Betrachten wir nun darin z als gegeben, so haben wir eine Gleichung 60[sten] Grades für x, die die Ikosaëdergleichung heisst.

Auf die Eigenschaften dieser Gleichung und ihre Beziehung zu der allgemeinen Gleichung 5[ten] Grades kommen wir in einem späteren Abschnitte zurück.

§. 61.

Die Invarianten des Ikosaëders.

Durch die Grundformen der Polyëdergruppen, die wir bisher kennen gelernt haben, ist, wie wir jetzt beweisen können, das Gebiet der Invarianten der betreffenden Gruppen erschöpft. Wir

beschränken uns bei diesem Beweise auf die Betrachtung der Ikosaëdergruppe, da für die anderen Gruppen ganz ähnliche Schlüsse zu machen sind, die wir dem Leser überlassen können. Der Umstand, dass bei der Tetraëder- und Octaëdergruppe neben den absoluten auch relative Invarianten vorkommen, während die Ikosaëdergruppe als einfache Gruppe nur absolute Invarianten hat, ist hierbei von keinem wesentlichen Einflusse.

Wir beweisen also, dass alle Invarianten der Ikosaëdergruppe sich als ganze rationale Functionen der drei Formen f, H, T darstellen lassen.

Dazu führt uns folgende Schlusskette:

1. Keine zwei der Ikosaëderformen f, H, T haben einen gemeinschaftlichen Theiler.

Dies folgt unmittelbar aus der Definition dieser Functionen, wonach die Gleichungen $f = 0$, $H = 0$, $T = 0$ die fünfzähligen, dreizähligen und zweizähligen Pole liefern, die alle von einander verschieden sind.

2. Eine Doppelwurzel der Ikosaëdergleichung

$$H^3 - zf^5 = 0 \tag{1}$$

ist nothwendig eine Wurzel von f, H oder T, und kann also nur für einen der Werthe $z = 0, \infty, 1728$ eintreten.

Wenn nämlich (1) eine Doppelwurzel hat, so müssen mit der Function zugleich die erste Ableitung, oder, wenn man die homogene Form anwendet, nach der Euler'schen Theorie [Bd. I, §. 17, (5)] die beiden Ableitungen nach x_1 und x_2 zugleich verschwinden, also

$$3H^2\, H'(x_1) - 5\,z\,f^4 f'(x_1) = 0,$$
$$3H^2\, H'(x_2) - 5\,z\,f^4 f'(x_2) = 0;$$

folglich bleiben, da H und f nach 1. nicht zugleich verschwinden, nur drei Möglichkeiten: entweder $H = 0$, $z = 0$, oder $f = 0$, $z = \infty$, oder endlich

$$H'(x_1)\,f'(x_2) - H'(x_2)\,f'(x_1) = 0,$$

d. h. $T = 0$, $z = 1728$ [§. 60, (4)]. Hieran schliesst sich auch der evidente Satz:

3. **Wenn $J(x_1, x_2)$ irgend eine invariante Form der Ikosaëdergruppe ist, und ξ eine ihrer Wurzeln, so dass $J(\xi, 1) = 0$ ist, so sind auch alle die Grössen Wurzeln von J, die aus ξ durch die gebrochenen Ikosaëdersubstitutionen hervorgehen.**

Wenn daher J mit einer der Functionen f, H, T einen Theiler gemein hat, so ist J durch die betreffende Form theilbar.

Wir denken uns nun zunächst aus J möglichst hohe Potenzen der drei Grundformen f, H, T weggehoben, so dass J zu diesen Functionen theilerfremd ist. Ist dann ξ eine Wurzel von J, so können wir η so bestimmen, dass ξ eine Wurzel der Form

$$\Theta = H^3 - \eta f^5$$

ist, und ξ ist dann nach 2. eine einfache Wurzel von Θ. Es müssen dann auch nach 3. alle übrigen Wurzeln von Θ zugleich Wurzeln von J sein, d. h. J ist durch Θ theilbar. Der Quotient ist wieder eine invariante Form des Ikosaëders, und der Schluss lässt sich wiederholen. Wir kommen so zu dem Satze:

4. Jede Invariante des Ikosaëders lässt sich in der Form darstellen:

$$J(x_1, x_2) = C f^\alpha H^\beta T^\gamma F(H^3, f^5), \tag{2}$$

worin α, β, γ nicht negative ganze Zahlen, C eine Constante und F eine ganze homogene Function bedeuten.

§. 62.

Polyëdergruppen der zweiten Art. Krystallographische Gruppen.

Wir haben schon im §. 51 auf Gruppen linearer ternärer Substitutionen aufmerksam gemacht, die ausser den eigentlichen auch uneigentlich orthogonale Substitutionen enthalten, und die wir Gruppen der zweiten Art nennen.

Wir wollen die endlichen unter ihnen jetzt als Polyëdergruppen der zweiten Art oder auch als erweiterte Polyëdergruppen, und die darin enthaltenen Substitutionen mit der

Determinante — 1 als Substitutionen der zweiten Art bezeichnen.

Nach den Resultaten des §. 50 sind diese Gruppen isomorph mit den Gruppen binärer linearer Substitutionen mit der Determinante + 1 und — 1, während bei den gebrochenen Substitutionen, die uns auf die Polyëdergruppen geführt haben, die beiden Arten nicht unterscheidbar sind.

Die endlichen Gruppen der zweiten Art sind, abgesehen von ihrem allgemeinen gruppentheoretischen Interesse, wichtig wegen ihrer Anwendung in der Krystallographie. Ihre vollständige Bestimmung bietet jetzt keine wesentlichen Schwierigkeiten mehr. Wir verstehen unter Substitutionen schlechtweg binäre lineare Substitutionen mit der Determinante ± 1, und erinnern daran, dass zwei solche Substitutionen, deren Coëfficienten sich nur durch das gemeinschaftliche Vorzeichen unterscheiden, wie

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}, \quad \begin{pmatrix}-\alpha, -\beta\\ -\gamma, -\delta\end{pmatrix},$$

als nicht verschieden gelten (§. 49).

Da eine Gruppe linearer Substitutionen die identische Substitution enthält, die von der Determinante + 1 ist, so müssen in jeder Gruppe Q der zweiten Art neben den uneigentlichen auch eigentliche Substitutionen vorkommen, und diese eigentlichen Substitutionen bilden für sich eine Gruppe P. Ist φ irgend eine in Q vorkommende Substitution der zweiten Art, so kommt jede Composition von φ mit einer Substitution aus Q der zweiten Art in P vor, und daher können wir Q immer so zerlegen:

(1) $$Q = P + P\varphi.$$

Die Gruppe P muss eine der früher betrachteten Polyëdergruppen sein. Es muss $\varphi^{-1} P \varphi = P$ sein, und P ist also ein Normaltheiler von Q. Ist umgekehrt P eine Polyëdergruppe und φ eine Substitution zweiter Art, die der Bedingung $\varphi^{-1} P \varphi = P$ genügt, so ist $Q = P + P\varphi$ eine Gruppe der zweiten Art.

Auch hier betrachten wir zwei Gruppen, die durch Transformation aus einander hervorgehen, als nicht wesentlich verschieden. Wir haben, um alle Q zu bilden, die verschiedenen Fälle durchzugehen.

I. Ist P die Einheitsgruppe, die wir als cyklische Gruppe ersten Grades mit C_1 bezeichnen, besteht also P nur aus der

identischen Substitution, so muss $\varphi^2 = 1$ sein, und dies ist auch ausreichend. Wir können hier durch Transformation φ auf die Form $\begin{pmatrix}\alpha, & 0 \\ 0, & -\alpha^{-1}\end{pmatrix}$ bringen und erhalten als Bedingung $\alpha^2 = \pm 1$, und demnach zwei Formen der Substitution φ:

$$\varphi' = \begin{pmatrix}i, & 0 \\ 0, & i\end{pmatrix}, \quad \varphi'' = \begin{pmatrix}1, & 0 \\ 0, & -1\end{pmatrix},$$

von denen der erste die Inversion, der zweite die Spiegelung genannt wird. Ueberträgt man sie nach §. 50, (1) auf eine rechtwinkelige Coordinatentransformation, so bedeutet φ' die gleichzeitige Vorzeichenänderung aller drei Coordinaten, φ'' die Vertauschung von x mit $-x$. Es ergeben sich hieraus die beiden Gruppen der zweiten Art:

$$(2) \qquad C_1' = \begin{pmatrix}i^h, & 0 \\ 0, & i^h\end{pmatrix}, \quad C_1'' = \begin{pmatrix}1, & 0 \\ 0, & (-1)^h\end{pmatrix}, \quad h = 0, 1.$$

II. Es sei P eine cyklische Gruppe C_n, $n > 1$.

Setzen wir

$$(3) \qquad c = \begin{pmatrix}\varepsilon, & 0 \\ 0, & \varepsilon^{-1}\end{pmatrix}, \quad \varepsilon = e^{\frac{\pi i}{n}},$$

so ist nach §. 55:

$$(4) \qquad C_n = 1, c, c^2, \ldots, c^{n-1},$$

worin

$$c^s = \begin{pmatrix}\varepsilon^s, & 0 \\ 0, & \varepsilon^{-s}\end{pmatrix};$$

wenn nun

$$(5) \qquad \varphi = \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}, \quad \alpha\delta - \beta\gamma = -1$$

ist, so bilden wir zunächst

$$(6) \qquad \varphi^{-1} c \varphi = \begin{pmatrix}\alpha\delta\varepsilon - \beta\gamma\varepsilon^{-1}, & \beta\delta(\varepsilon - \varepsilon^{-1}) \\ -\alpha\gamma(\varepsilon - \varepsilon^{-1}), & \alpha\delta\varepsilon^{-1} - \beta\gamma\varepsilon\end{pmatrix},$$

$$(7) \qquad \varphi^2 = \begin{pmatrix}\alpha^2 + \beta\gamma, & (\alpha+\delta)\beta \\ (\alpha+\delta)\gamma, & \beta\gamma + \delta^2\end{pmatrix}.$$

Diese beiden Substitutionen müssen in der Reihe (4) vorkommen, und es muss also $\beta\delta = 0$, $\alpha\gamma = 0$ sein; also müssen entweder β und γ oder α und $\delta = 0$ sein. Ist $\beta = \gamma = 0$, so folgt aus (7), dass α von der Form $\varepsilon^{1/2 r}$, also

$$\varphi = \begin{pmatrix}e^{\frac{\pi i}{2n} r}, & 0 \\ 0, & -e^{-\frac{\pi i}{2n} r}\end{pmatrix}$$

sein muss, worin r eine ganze Zahl bedeutet. Je nachdem r ungerade oder gerade angenommen wird, erhalten wir zwei verschiedene Gruppen, die sich nicht durch Transformation auf einander zurückführen lassen:

$$1) \qquad C'_n = \begin{pmatrix} e^{\frac{\pi i h}{2n}}, & 0 \\ 0, & (-1)^h e^{-\frac{\pi i h}{2n}} \end{pmatrix} \quad h = 0, 1, \ldots, 2n-1,$$

$$2) \qquad C''_n = \begin{pmatrix} e^{\frac{\pi i h}{n}}, & 0 \\ 0, & \pm e^{-\frac{\pi i h}{n}} \end{pmatrix} \quad h = 0, 1, \ldots, n-1. \quad \text{(beide Vorzeichen)}$$

Wenn n gerade ist, so kommen C'_1 und C''_1 beide unter C''_n vor; ist aber n ungerade, so kommt C'_1 in C'_n, C''_1 in C''_n vor.

Ist sodann $\alpha = \delta = 0$, $\beta\gamma = 1$, so können wir φ durch die Transformation

$$\begin{pmatrix} \beta^{-\frac{1}{2}}, & 0 \\ 0, & \beta^{\frac{1}{2}} \end{pmatrix} \begin{pmatrix} 0, & \beta \\ \gamma, & 0 \end{pmatrix} \begin{pmatrix} \beta^{\frac{1}{2}}, & 0 \\ 0, & \beta^{-\frac{1}{2}} \end{pmatrix} = \begin{pmatrix} 0, & 1 \\ 1, & 0 \end{pmatrix},$$

durch die die Gruppe P ungeändert bleibt, umformen, und erhalten noch eine dritte Gruppe:

$$3) \qquad C'''_n = \begin{pmatrix} e^{\frac{\pi i h}{n}}, & 0 \\ 0, & e^{-\frac{\pi i h}{n}} \end{pmatrix}, \quad \begin{pmatrix} 0, & e^{\frac{\pi i h}{n}} \\ e^{-\frac{\pi i h}{n}}, & 0 \end{pmatrix}$$
$$h = 0, 1, \ldots, n-1.$$

III. Es sei P die Diëdergruppe D_n, die aus den Substitutionen

$$(8) \qquad \begin{aligned} D_n = {} & 1,\ c,\ c^2,\ \ldots,\ c^{n-1} \\ & d,\ cd,\ c^2 d,\ \ldots,\ c^{n-1} d \\ = {} & C_n + C_n d \end{aligned}, \quad d = \begin{pmatrix} 0, & i \\ i, & 0 \end{pmatrix}$$

besteht. Die Substitution c ist vom n^{ten}, die $c^\lambda d$ sind alle vom 2ten Grade. Es ist aber $\varphi^{-1} c \varphi$ vom n^{ten} Grade, und muss daher, wenn $n > 2$ ist, unter den Potenzen von c enthalten sein. Folglich sind zur Bestimmung von φ die vorigen Betrachtungen anwendbar, und in der Gruppe Q muss eine der Gruppen C'_n, C''_n, C'''_n enthalten sein. Da d nicht in diesen Gruppen vorkommt, so ergeben sich für die Diëdergruppen zweiter Art die Formen

$$(9) \qquad C'_n + C'_n d, \quad C''_n + C''_n d, \quad C'''_n + C'''_n d,$$

von denen die beiden ersten

$$1)\quad D'_n = \begin{pmatrix} e^{\frac{\pi i h}{2n}}, & 0 \\ 0, & (-1)^h e^{-\frac{\pi i h}{2n}} \end{pmatrix}, \quad \begin{pmatrix} 0, & -e^{\frac{\pi i h}{2n}} \\ (-1)^{h+n} e^{-\frac{\pi i h}{2n}}, & 0 \end{pmatrix}$$

$$h = 0, 1, \ldots, 2n - 1,$$

$$2)\quad D''_n = \begin{pmatrix} e^{\frac{\pi i h}{n}}, & 0 \\ 0, & \pm e^{-\frac{\pi i h}{n}} \end{pmatrix}, \quad \begin{pmatrix} 0, & e^{\frac{\pi i (2h+n)}{2n}} \\ \pm e^{-\frac{\pi i (2h+n)}{2n}}, & 0 \end{pmatrix}$$

$$h = 0, 1, \ldots, n - 1$$

sind, während die dritte Gruppe (9)

$$\begin{pmatrix} e^{\frac{\pi i h}{n}}, & 0 \\ 0, & e^{-\frac{\pi i h}{n}} \end{pmatrix}, \quad \begin{pmatrix} 0, & e^{\frac{\pi i h}{n}} \\ e^{-\frac{\pi i h}{n}}, & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0, & e^{\frac{\pi i}{2n}(2h+n)} \\ -e^{-\frac{\pi i}{2n}(2h+n)}, & 0 \end{pmatrix}, \quad \begin{pmatrix} e^{\frac{\pi i}{2n}(2h+n)}, & 0 \\ 0, & -e^{-\frac{\pi i}{2n}(2h+n)} \end{pmatrix}$$

$$h = 0, 1, \ldots, n - 1$$

ergiebt, was bei geradem n mit D''_n, bei ungeradem n mit D'_n übereinstimmt.

Der Fall $n = 2$, wo $c = \begin{pmatrix} i, & 0 \\ 0, & -i \end{pmatrix}$ ist, bildet nur eine scheinbare Ausnahme, weil in diesem Falle

$$(10)\qquad \varphi^{-1} c \varphi = d \quad \text{oder} \quad \varphi^{-1} c \varphi = c d$$

sein kann. Verfolgt man diese Annahmen durch einfache Rechnung, so ergeben sich noch zwei Gruppen:

$$(11)\qquad \begin{matrix} 1, & c, & d, & c d, & \varphi_1, & \varphi_1 c, & \varphi_1 d, & \varphi_1 c d \\ 1, & c, & d, & c d, & \varphi_2, & \varphi_2 c, & \varphi_2 d, & \varphi_2 c d, \end{matrix}$$

worin

$$\varphi_1 = \begin{pmatrix} \frac{1}{\sqrt{2}}, & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}, & \frac{-1}{\sqrt{2}} \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} \frac{1}{\sqrt{2}}, & -\frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}}, & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

Es ist aber

$$\varphi_2^{-1}\varphi_1\varphi_2 = \begin{pmatrix} 0, & e^{\frac{\pi i}{4}} \\ e^{-\frac{\pi i}{4}}, & 0 \end{pmatrix}$$

$$\varphi_1^{-1}\varphi_2\varphi_1 = \begin{pmatrix} 0, & e^{\frac{\pi i}{4}} \\ e^{-\frac{\pi i}{4}}, & 0 \end{pmatrix},$$

$$c\varphi_1 = \varphi_1 d, \quad d\varphi_1 = \varphi_1 c, \quad cd\varphi_1 = \varphi_1 dc$$
$$c\varphi_2 = \varphi_2 dc, \quad d\varphi_2 = \varphi_2 d, \quad cd\varphi_2 = \varphi_2 c,$$

und aus diesen Formeln folgt, dass die Gruppen (11) durch Transformation mit φ_1 und φ_2 in D_2' transformirt werden.

Bei der Bestimmung der übrigen Polyëdergruppen zweiter Art sind die folgenden allgemeinen Bemerkungen von Nutzen. Die Inversion $j = \begin{pmatrix} i, & 0 \\ 0, & i \end{pmatrix}$ ist eine Aehnlichkeitssubstitution (§. 37) und daher mit jeder anderen Substitution vertauschbar, und folglich können wir aus jeder Polyëdergruppe erster Art wenigstens eine Gruppe zweiter Art herleiten:

$$P + Pj. \tag{12}$$

Um die anderen etwa noch vorhandenen Gruppen dieser Art zu finden, erinnern wir uns, dass nach dem Sylow'schen Satze (§. 29, I.) in jeder Gruppe G eine Gruppe enthalten sein muss, deren Grad die höchste Potenz von 2 ist, die im Grade von G aufgeht. Die erweiterten Tetraëder-, Octaëder- und Ikosaëdergruppen haben aber die Grade 24, 48, 120, müssen also einen Theiler vom Grade 8, 16, 8 enthalten.

Es sei nun T die Tetraëder-, O die Octaëder- und J die Ikosaëdergruppe. In T und J ist eine Vierergruppe D_2 enthalten, aber keine Substitution vierter Ordnung, in O eine Diëdergruppe D_4 und keine Substitution achter Ordnung, und es muss daher unter den erweiterten Polyëdergruppen eine der unter III. betrachteten erweiterten Diëdergruppen enthalten sein.

Von den erweiterten Diëdergruppen entsteht aber D_2'' aus D_2 durch Inversion, während

$$D_2' = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \begin{pmatrix} \sqrt{i}, & 0 \\ 0, & +i\sqrt{i} \end{pmatrix}, \begin{pmatrix} i, & 0 \\ 0, & -i \end{pmatrix}, \begin{pmatrix} i\sqrt{i}, & 0 \\ 0, & +\sqrt{i} \end{pmatrix},$$
$$\begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}, \begin{pmatrix} 0, & -i\sqrt{i} \\ \sqrt{i}, & 0 \end{pmatrix}, \begin{pmatrix} 0, & i \\ i, & 0 \end{pmatrix}, \begin{pmatrix} 0, & -\sqrt{i} \\ i\sqrt{i}, & 0 \end{pmatrix}$$

durch Composition von D_2 mit

$$j_1 = \begin{pmatrix} 0, & -\sqrt{i} \\ i\sqrt{i}, & 0 \end{pmatrix}$$

entsteht, also

$$D_2' = D_2 + D_2 j_1$$

ergiebt. Nun ist allgemein:

$$j_1^{-1} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} j_1 = \begin{pmatrix} \delta, & \gamma i \\ -\beta i, & \alpha \end{pmatrix},$$

und daraus schliesst man nach §. 56, (4), dass $j_1^{-1} T j_1 = T$ ist, dass also aus der Tetraëdergruppe zwei erweiterte Gruppen $T' = T + Tj$ und $T'' = T + Tj_1$ abgeleitet werden können; aber auch nur zwei, weil nach §. 56 die Tetraëdergruppe durch eine darin enthaltene Vierergruppe völlig bestimmt ist. Denn wenn wir statt der Erweiterung D_2' die Erweiterung der Vierergruppe zu einer der Gruppen (11) wählen, so erhalten wir eine erweiterte Tetraëdergruppe T''', die durch Transformation mit φ_1 oder φ_2 in T'' übergeht.

Da die Substitution

$$\begin{pmatrix} 0, & e^{\frac{\pi i}{8}} \\ e^{-\frac{\pi i}{8}}, & 0 \end{pmatrix}$$

mit der Octaëdergruppe §. 57, (8) nicht vertauschbar ist, so lässt sich aus der Octaëdergruppe ausser durch Inversion keine weitere Gruppe zweiter Art ableiten, und dasselbe gilt von der Ikosaëdergruppe. Man muss, um diese Schlussweise anzuwenden, die Ikosaëdergruppe so transformiren, dass eine der darin enthaltenen Vierergruppen die einfachste Gestalt annimmt, was etwas weitläufig, aber durchaus nicht schwierig ist, und hier nicht weiter ausgeführt werden soll.

Wir erhalten also noch folgende Gruppen zweiter Art:

IV. 1) $T' = T + Tj$, 2) $T'' = T + Tj_1$.

V. $O' = O + Oj$.

IV. $J' = J + Jj$.

Hierin sind die 32 Symmetriesysteme der Krystallographen ıthalten. Es sind die Gruppen:

$C_1,\ C_1',\ C_1''$	$D_2,\ D_2',\ D_2''$
$C_2,\ C_2',\ C_2'',\ C_2'''$	$D_3,\ D_3',\ D_3''$
$C_3,\ C_3',\ C_3'',\ C_3'''$	$D_4,\ D_4'$
$C_4,\ C_4',\ C_4''$	$D_6,\ D_6'$
$C_6,\ C_6',\ C_6''$	$T,\ T',\ T''$
	$O,\ O'.$

Die übrigen Polyëdergruppen sind in der Krystallographie urch das krystallographische Gesetz der rationalen Indices aus-eschlossen [1]).

[1]) Vgl. Schönfliess, Krystallsysteme u. Krystallstructur. Leipzig 1891.

Neunter Abschnitt.

Congruenzgruppen.

---

§. 63.

Functionen-Congruenzen.

Aus den linearen Substitutionen, deren Bildung und Zusammensetzung wir in den früheren Abschnitten kennen gelernt haben, lassen sich noch eine ganz andere Art endlicher Gruppen ableiten, die Congruenzgruppen.

Diese Congruenzgruppen haben ein mannigfaches Interesse. Sie stammen zunächst aus der Theorie der elliptischen Functionen, wo sie sich als Galois'sche Gruppen der Modulargleichungen einstellen. Sie sind aber auch für die allgemeine Gruppentheorie von Wichtigkeit, weil sie uns ein Mittel geben, ganze Reihen von einfachen Gruppen zu bilden. Dies ist um so bemerkenswerther, als, wie wir im vierten Abschnitte gesehen haben, die einfachen Gruppen, wenigstens unter den niedrigeren Gradzahlen, sehr selten sind.

Die Theorie dieser Congruenzgruppen wird nicht nur ausserordentlich verallgemeinert, sondern die herrschenden Gesetze treten weit schärfer hervor, wenn man sich auf eine von Gauss herrührende Erweiterung des Congruenzbegriffes stützt, die seitdem mehrfach für die Probleme der Gruppentheorie, besonders von Galois, ausgebildet und angewandt worden ist[1]).

---

[1]) Galois, „Sur la théorie des nombres". Bulletin des sciences math. de Ferussac. 1830. (Vergl. die Note zu §. 151 des ersten Bandes.) — Schönemann, Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modulus eine reelle Primzahl ist. (Crelle's Journ. f. Mathematik, Bd. 31, 1846.) — Dedekind, Abriss einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahlmodulus. (Crelle's Journ. f. Mathematik, Bd. 54, 1856.)

Um eine Grundlage für diese Theorie zu gewinnen, betrachten wir eine ganze Function einer veränderlichen Grösse t

(1) $$f(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n,$$

deren Coëfficienten ganze Zahlen sein sollen. Wir wählen ausserdem eine Primzahl p als Modulus, und nehmen an, a_0 sei durch p nicht theilbar.

Zwei ganze Functionen von t, in denen entsprechende Coëfficienten nach dem Modul p congruent sind, sollen selbst nach dem Modul p congruent genannt werden.

Die Function $f(t)$ heisst nach dem Modul p reducibel, wenn es zwei ganze ganzzahlige Functionen $\varphi(t)$, $\psi(t)$ giebt, in deren jeder wenigstens ein von t abhängiges Glied einen durch p nicht theilbaren Coëfficienten hat, so dass

(2) $$f(t) \equiv \varphi(t)\, \psi(t) \pmod p$$

ist. In $\varphi(t)$ und $\psi(t)$ kann man alle Glieder, deren Coëfficienten durch p theilbar sind, weglassen, und dann muss der Grad von $\varphi(t)\, \psi(t)$ mit dem Grade von $f(t)$ übereinstimmen. Es müssen also die Grade von $\varphi(t)$ und $\psi(t)$ niedriger als n sein. Giebt es keine solche Functionen $\varphi(t)$, $\psi(t)$, so heisst $f(t)$ nach dem Modul p irreducibel.

Eine nach dem Modul p irreducible Function ist gewiss immer im Körper der rationalen Zahlen absolut irreducibel. Das Umgekehrte ist aber nicht nothwendig.

So ist z. B. die Function 2ten Grades $t^2 - R$ reducibel nach p, wenn R quadratischer Rest von p ist; denn ist $a^2 \equiv R \pmod p$, so ist

$$t^2 - R \equiv (t - a)(t + a) \pmod p.$$

Dagegen ist $t^2 - N$, wenn N Nichtrest von p ist, irreducibel, weil sonst $t^2 - N$ für ein rationales t durch p theilbar werden müsste.

Ein anderes Beispiel bieten die Functionen

$$t^2 + t + 1, \quad t^3 + t + 1,$$

die für den Modul 2 irreducibel sind. Denn wären sie reducibel, so müsste einer der Factoren linear sein, und es müsste eine ganze Zahl geben, die, für t eingesetzt, diese Functionen zu geraden Zahlen macht. Das aber ist offenbar unmöglich, da beide Functionen für $t = 0$ und $t = 1$ ungerade Zahlen sind.

Bedeutet

(3) $$P = t^n + p_1 t^{n-1} + p_2 t^{n-2} + \cdots + p_{n-1} t + p_n$$

eine nach dem Modul p irreducible Function n^{ten} Grades, in der wir der Einfachheit halber den Coëfficienten der höchsten Potenz t^n gleich 1 annehmen, so lässt sich aus jeder anderen ganzen Function $F(t)$ mit ganzzahligen Coëfficienten ein Rest $\Phi(t)$ ableiten, dessen Grad niedriger als n ist, indem man (nach §. 3 des ersten Bandes)

(4) $$F(t) = QP + \Phi(t)$$

setzt. $\Phi(t)$ hat hierin ganzzahlige Coëfficienten, und wir bezeichnen ihre Beziehung zur Function $F(t)$ als eine Congruenz nach dem Modul P.

Es heissen also zwei Functionen $F(t)$, $F_1(t)$, die denselben Rest $\Phi(t)$ haben, congruent nach dem Modul P, was durch die Formel

$$F(t) \equiv F_1(t) \pmod{P}$$

ausgedrückt wird. Damit ist gleichbedeutend, dass $F(t) - F_1(t)$ durch P theilbar ist.

Wenn zwei Functionen $F(t)$ und $F_1(t)$ nicht gleichen Rest geben, sondern zwei Reste, die nach dem Modul p congruent sind, so heissen die Functionen F, F_1 congruent nach dem Doppelmodul P, p, und man drückt dies durch eine Formel so aus:

(5) $$F(t) \equiv F_1(t) \pmod{P, p}.$$

Für diese Art der Congruenz gilt der Satz:

1. Das Product zweier Functionen $F(t)$, $F_1(t)$ kann nicht mit Null congruent sein, wenn nicht der eine Factor mit Null congruent ist.

Der Beweis ergiebt sich aus dem Algorithmus des grössten gemeinschaftlichen Theilers. Ist nämlich P_1 eine ganze Function von niedrigerem Grade als P, die nicht nach dem Modul p mit Null congruent ist, so kann man eine Reihe von eben solchen Functionen P_2, P_3, ... von abnehmendem Grade, und die Quotienten Q_1, Q_2, ... gleichfalls als ganze Functionen so bestimmen, dass

(6) $$P \equiv Q_1 P_1 + P_2, \quad P_1 \equiv Q_2 P_2 + P_3, \ldots,$$
$$P_{\nu-2} \equiv Q_{\nu-1} P_{\nu-1} + P_\nu \pmod{p}$$

wird, und die Reihe dieser Gleichungen bricht ab, wenn P_ν eine Constante (ganze Zahl) geworden ist. Diese Constante P_ν kann

aber nicht $\equiv 0 \pmod{p}$ sein; denn sonst liesse sich aus (6) eine Congruenz ableiten:

$$P \equiv T P_{\nu-1} \pmod{p},$$

in der T eine nicht constante Function von t ist, und P wäre nicht irreducibel nach dem Modul p.

Ist nun Q irgend eine ganze Function von t, die der Bedingung

$$Q P_1 \equiv 0 \pmod{P, p}$$

genügt, so folgt aus (6) durch Multiplication mit Q:

$$Q P_2 \equiv 0,\ Q P_3 \equiv 0, \ldots, Q P_\nu \equiv 0 \pmod{P, p},$$

also $Q \equiv 0$. Und wenn wir also für P_1, Q die Reste der Functionen $F(t)$, $F_1(t)$ setzen, so ist hiermit der Satz 1. bewiesen.

Die Reste aller Functionen $F(t)$ nach dem Modul P sind von der Form

(7) $$X = X(t) = x_0 + x_1 t + \cdots + x_{n-1} t^{n-1},$$

und wenn man nur die nach dem Modul p incongruenten unter ihnen haben will, so genügt es, die Coëfficienten $x_0, x_1, \ldots x_{n-1}$ die Reihe der Zahlen $0, 1, 2, \ldots, p-1$ durchlaufen zu lassen.

Es giebt also p^n und nicht mehr nach den Moduln P, p incongruente Functionen.

§. 64.

Congruenzkörper.

Es ist nur eine andere Ausdrucksweise für die im vorigen Paragraphen durchgeführten Betrachtungen, wenn man mit Galois eine imaginäre Zahl ε einführt, die der Congruenz

(1) $$P(\varepsilon) \equiv 0 \pmod{p}$$

genügt. Eine ganze rationale Zahl dieser Art giebt es nicht, sobald $n > 1$ ist, weil sonst $P(t) - P(\varepsilon) = (t - \varepsilon)\, Q$ durch $t - \varepsilon$ theilbar, mithin $P(t) \equiv (t - \varepsilon)\, Q$, und $P(t)$ nicht irreducibel wäre. Gleichwohl kann man, wie man in der gewöhnlichen Zahlenlehre die imaginäre Einheit $i = \sqrt{-1}$ einführt, ein solches Symbol ε in der Rechnung benutzen. Man rechnet damit, sofern es sich um Addition, Subtraction und Multiplication handelt, nach den Regeln der Buchstabenrechnung, und kann dabei nach Belieben die Gleichung $P(\varepsilon) = 0$ benutzen. Man kann sogar unter ε geradezu eine Wurzel der Gleichung $P(x) = 0$

im gewöhnlichen Sinne verstehen. Alle Zahlen, auf die man hierbei kommt, lassen sich auf die Form

$$\alpha = a_0 + a_1 \varepsilon + \cdots + a_{n-1} \varepsilon^{n-1} \tag{2}$$

bringen. Da bei der Rechnung mit solchen Zahlen der Modul p immer festgehalten wird, so wollen wir zwei Zahlen, die nach dem Modul p congruent sind, geradezu als gleich bezeichnen. Objecte der Rechnung sind dann eigentlich nicht die einzelnen Zahlen selbst, sondern die aus allen unter einander congruenten Zahlen bestehenden Zahlclassen. Diese Zahlen α werden die Galois'schen Imaginären genannt. Das zu einem bestimmten ε gehörige System solcher imaginärer Zahlen bezeichnen wir der Abkürzung wegen mit $\mathfrak{E}$.

Wir haben dann zunächst den Satz:

2. Es giebt p^n und nicht mehr verschiedene Zahlen in $\mathfrak{E}$.

Aus dem Satze 1. aber folgt noch:

3. Das Product von zwei oder mehr Zahlen aus $\mathfrak{E}$ ist dann und nur dann gleich Null, wenn wenigstens einer der Factoren gleich Null ist.

Wir erhalten das vollständige Zahlensystem $\mathfrak{E}$, wenn man die rationalen Zahlen $a_0, a_1, \ldots, a_{n-1}$ in (2) je ein volles Restsystem nach dem Modul p durchlaufen lässt. Jedes System $\mathfrak{E}$ enthält die Reste der natürlichen Zahlen $0, 1, \ldots, p-1$, und für $n = 1$ ist $\mathfrak{E}$ mit diesem Systeme identisch.

Ist α eine feste von Null verschiedene Zahl in $\mathfrak{E}$, so durchläuft $\alpha\xi$ zugleich mit ξ das volle System $\mathfrak{E}$. Denn aus 3. folgt, dass $\alpha\xi$ nur dann gleich $\alpha\xi'$ sein kann, wenn $\xi = \xi'$ ist. Daraus folgt:

4. Sind α, β zwei gegebene Zahlen in $\mathfrak{E}$ und α von Null verschieden, so giebt es eine und nur eine Zahl γ in $\mathfrak{E}$, die der Bedingung

$$\alpha\gamma = \beta$$

genügt.

Damit ist auch die Operation der Division in dem Systeme $\mathfrak{E}$ als erlaubt nachgewiesen. Wir bezeichnen die Zahl γ, deren Existenz in 4. ausgesprochen ist, mit

$$\beta : \alpha \quad \text{oder} \quad \frac{\beta}{\alpha}.$$

Man kann das System $\mathfrak{C}$ einen endlichen Körper nennen, da es nur eine endliche Anzahl von Zahlen enthält, die das charakteristische Merkmal eines Körpers, nämlich die unbeschränkte Ausführbarkeit der Rechenoperationen, ausgenommen die Division durch Null, aufweisen (Bd. I, §. 139)[1]). Wir wollen daher $\mathfrak{C}$ einen Congruenzkörper nennen.

Es soll n der Grad und p der Modul des Körpers $\mathfrak{C}$ heissen.

Ist α eine von Null verschiedene Zahl in $\mathfrak{C}$, so durchläuft das Product $\alpha \xi = \eta$ zugleich mit ξ das volle Zahlensystem $\mathfrak{C}$. Schliessen wir $\xi = 0$ aus, so kommt auch $\eta = 0$ nicht vor, und das Product Π aller ξ stimmt mit dem Producte aller η überein und ist von Null verschieden. Durch Multiplication aller Gleichungen $\alpha \xi = \eta$ folgt aber

$$\alpha^{p^n - 1} \Pi = \Pi,$$

und nach Abwerfung des gemeinsamen Factors Π ergiebt sich

5. der Fermat'sche Satz:

$$\alpha^{p^n - 1} = 1. \tag{3}$$

Multiplicirt man mit α, so erhält man diesen Satz in der Form

$$\alpha^{p^n} = \alpha, \tag{4}$$

in der er auch noch für $\alpha = 0$ besteht. Ist α von Null verschieden, so giebt es wegen (3) einen kleinsten positiven Exponenten e, für den

$$\alpha^e = 1 \tag{5}$$

ist, und für den folglich die Potenzen $1, \alpha, \alpha^2, \ldots, \alpha^{e-1}$ von einander verschieden sind. Man sagt dann, α gehört zum Exponenten e. Dieser Exponent e muss ein Theiler von $p^n - 1$ sein. Denn ist $\alpha^m = 1$ für irgend einen Exponenten m, so setzen wir $m = qe + e'$, worin q eine ganze Zahl und $e' < e$ ist. Dann ist auch $\alpha^{e'} = 1$, und folglich muss $e' = 0$, d. h. m durch e theilbar sein. Unter diesen Exponenten m findet sich auch $p^n - 1$. Setzen wir also

$$p^n - 1 = ef,$$

so wird α^h immer dann zum Exponenten e gehören, wenn h relativ prim zu e ist. Denn dann und nur dann ist he das kleinste positive, durch e theilbare Vielfache von h.

---

[1]) Man sehe des Verfassers Abhandlung: Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie. Mathematische Annalen, Bd. 43.

Giebt es also überhaupt eine zum Exponenten e gehörige Zahl α, so giebt es so viele wie relative Primzahlen zu e, die positiv und kleiner als e sind, eine Zahl, die wir schon früher mit $\varphi(e)$ bezeichnet haben, und die, wenn e alle Divisoren von $p^n - 1$ durchläuft, der Relation

$$(6) \qquad \Sigma\, \varphi(e) = p^n - 1$$

genügt (Bd. I, §. 132, 133).

Ist $\psi(e)$ die Anzahl der Zahlen α, die zum Exponenten e gehören, so ist $\psi(e) = \varphi(e)$ oder $= 0$, und da die Anzahl aller Zahlen α gleich $p^n - 1$ ist und jede Zahl α zu einem und nur zu einem Exponenten gehört, so ist auch

$$(7) \qquad \Sigma\, \psi(e) = p^n - 1,$$

und aus (6) und (7) folgt, dass $\psi(e)$ immer gleich $\varphi(e)$ ist.

Es giebt also $\varphi(p^n - 1)$ Zahlen γ in $\mathfrak{E}$, die zum Exponenten $p^n - 1$ gehören, und die folglich die Eigenschaft haben, dass die Potenzen

$$(8) \qquad 1, \gamma, \gamma^2, \ldots, \gamma^{p^n - 2}$$

alle von einander verschieden sind. Durch diese Reihe ist daher die Gesammtheit der von Null verschiedenen Zahlen in $\mathfrak{E}$ erschöpft.

Solche Zahlen γ heissen primitive Wurzeln von $\mathfrak{E}$.

Unter den Zahlen in $\mathfrak{E}$ giebt es solche, die als Quadrat einer anderen Zahl in $\mathfrak{E}$ darstellbar sind, die wir Quadrate nennen, und andere, bei denen dies nicht zutrifft, die wir Nichtquadrate nennen.

Wenn $p = 2$ ist, so ist jede Zahl in $\mathfrak{E}$ ein Quadrat, wie die Formel (4) zeigt.

Wenn aber p ungerade ist, so besteht die eine Hälfte der von Null verschiedenen Zahlen in $\mathfrak{E}$ aus Quadraten, die andere aus Nichtquadraten.

Denn zwei entgegengesetzte Zahlen, wie $+\alpha$ und $-\alpha$, sind bei ungeradem p von einander verschieden, und geben trotzdem dasselbe Quadrat. Wenn man also die sämmtlichen Zahlen von $\mathfrak{E}$ zum Quadrat erhebt, so erhält man höchstens $\frac{1}{2}(p^n - 1)$ verschiedene Quadrate. Nun kann andererseits β^2 nur dann gleich α^2 sein, wenn $\beta = \pm \alpha$ ist; denn aus $\beta^2 - \alpha^2 = (\beta - \alpha)(\beta + \alpha) = 0$ folgt, dass $\beta - \alpha$ oder $\beta + \alpha$ verschwinden muss. Es giebt also wirklich $\frac{1}{2}(p^n - 1)$ Quadrate und ebenso viele Nichtquadrate.

Wenn man die Null mit zu den Quadraten zählt, so erhält man den Satz:

6. Wenn $p = 2$ ist, so sind alle Zahlen in $\mathfrak{E}$ Quadrate. Ist p ungerade, so giebt es $1/2\,(p^n + 1)$ Quadrate, $1/2\,(p^n - 1)$ Nichtquadrate in $\mathfrak{E}$.

Bei ungeradem p muss eine primitive Wurzel immer ein Nichtquadrat sein und in der Reihe (8) sind die Zahlen mit geraden Exponenten die Quadrate, die mit ungeraden Exponenten die Nichtquadrate.

Das Product und der Quotient zweier Quadrate ist offenbar wieder ein Quadrat.

Daraus folgt, dass das Product aus einem Nichtquadrat und einem von Null verschiedenen Quadrate ein Nichtquadrat ist. Denn ist das Product $\alpha\beta$ ein Quadrat und der eine Factor α ein Quadrat, so muss auch $\beta = \alpha\beta : \alpha$ ein Quadrat sein.

Weiter schliesst man daraus, dass das Product von zwei Nichtquadraten ein Quadrat ist. Denn bedeutet β irgend ein Nichtquadrat, so lasse man in dem Producte $\beta\xi$ den Factor ξ die sämmtlichen von Null verschiedenen Zahlen von $\mathfrak{E}$ durchlaufen. Das Product durchläuft dann dieselbe Zahlenreihe, und da für alle quadratischen ξ das Product $\beta\xi$ Nichtquadrat ist, so muss es für die nichtquadratischen ξ Quadrat sein.

Alles dies ergiebt sich auch sehr einfach aus der Darstellung (8) der Zahlen von $\mathfrak{E}$ durch eine primitive Wurzel.

Wir schliessen diese allgemeinen Betrachtungen mit dem Satze, den wir später brauchen werden:

7. Jede nicht quadratische Zahl ist die Summe von zwei Quadraten.

Hierbei ist p als ungerade vorauszusetzen, da es nur dann nichtquadratische Zahlen giebt.

Es lässt sich dann zunächst jede Zahl β als Differenz zweier Quadrate darstellen, wie die Identität

$$(\beta + 1/4)^2 - (\beta - 1/4)^2 = \beta$$

zeigt. Ist nun -1 ein Quadrat in $\mathfrak{E}$, so setze man

$$(\beta + 1/4)^2 = \xi^2, \quad -(\beta - 1/4)^2 = \eta^2,$$

und erhält

$$\beta = \xi^2 + \eta^2.$$

Ist aber -1 und also auch $p - 1$ Nichtquadrat, so suche man in der Reihe der natürlichen Zahlen $1, 2, \ldots, p-1$, deren

erstes Glied ein Quadrat und deren letztes ein Nichtquadrat ist, ein quadratisches Glied auf, auf welches ein Nichtquadrat folgt.

Ist dann also $a = \xi^2$ ein Quadrat und $\xi^2 + 1$ ein Nichtquadrat, so ist, wenn β ein Nichtquadrat ist, $\beta : \xi^2 + 1 = \eta^2$ ein Quadrat, und daraus folgt:

$$\beta = \xi^2 \eta^2 + \eta^2$$

w. z. b. w.

§. 65.

Congruenzgruppen im Körper $\mathfrak{C}$.

In jedem Congruenzkörper $\mathfrak{C}$ kann man eine endliche Gruppe von linearen Substitutionen bilden, wenn man in

(1) $$A = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

die Elemente $\alpha, \beta, \gamma, \delta$ alle Zahlen von $\mathfrak{C}$ durchlaufen lässt, und wenn man je zwei dieser Substitutionen nach der Vorschrift

(2) $$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \beta\gamma', & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma', & \gamma\beta' + \delta\delta' \end{pmatrix}$$

componirt. Der Grad dieser Gruppe ist p^{4n}, wenn p der Modul und n der Grad von $\mathfrak{C}$ ist.

Darin ist aber eine Gruppe niedrigeren Grades enthalten. Nennen wir $\alpha\delta - \beta\gamma$ die Determinante der Substitution (1), so folgt aus (2), dass die Determinante der aus A und A' componirten Substitution AA' gleich dem Producte der Determinanten von A und A' ist. Wenn wir daher den Zahlen $\alpha, \beta, \gamma, \delta$ die Bedingung auferlegen, dass

(3) $$\alpha\delta - \beta\gamma = 1$$

sein soll, so bilden auch diese Elemente A eine Gruppe. Der Grad dieser Gruppe ist gleich der Anzahl der Lösungen von (3). Um diese Anzahl zu finden, bemerken wir zunächst, dass wir für α, β irgend zwei Zahlen aus $\mathfrak{C}$ setzen können, die nicht beide gleich Null sind. Denn ist etwa α von Null verschieden, so kann man $\gamma = 0$, $\delta = 1 : \alpha$ setzen und hat so die Bedingung (3) erfüllt. Die Anzahl der brauchbaren Zahlenpaare α, β ist also $p^{2n} - 1$. Hat man aber zu einem Zahlenpaare α, β eine Lösung γ_0, δ_0 von (3) gefunden, so müssen alle übrigen der Bedingung

$$\alpha(\delta - \delta_0) = \beta(\gamma - \gamma_0)$$

genügen, und wenn man also $\gamma - \gamma_0 = \alpha \xi$ setzt (falls α von Null verschieden ist), so folgt $\delta - \delta_0 = \beta \xi$, also

$$\gamma = \gamma_0 + \alpha \xi, \quad \delta = \delta_0 + \beta \xi,$$

und umgekehrt genügt auch jedes in dieser Form enthaltene Zahlenpaar γ, δ. Dies gilt offenbar auch noch in dem ausgenommenen Falle $\alpha = 0$. Da wir nun p^n verschiedene Zahlen für ξ setzen können, so ergiebt sich der Grad unserer Gruppe gleich

$$p^n (p^{2n} - 1). \tag{4}$$

Ist p ungerade, so können wir eine noch kleinere Gruppe ableiten:

Ist nämlich $p = 2$, so ist eine Zahl α von $-\alpha$ nicht verschieden, es sind also auch die Elemente

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \quad \begin{pmatrix} -\alpha, & -\beta \\ -\gamma, & -\delta \end{pmatrix} \tag{5}$$

mit einander identisch. Wenn aber p ungerade ist, so sind die beiden Elemente (5) von einander verschieden, und das ganze System dieser Substitutionen zerfällt in Paare von der Form (5).

Wenn wir zwei solche Paare nehmen und componiren je ein Element des einen Paares mit je einem Element des anderen nach der Regel (2), so erhalten wir nur zwei verschiedene Elemente, die wieder ein solches Paar bilden. Diese Paare können also selbst als Elemente einer neuen Gruppe vom Grade

$$\frac{p^n (p^{2n} - 1)}{2} \tag{6}$$

aufgefasst werden. Wir können uns auch so ausdrücken, dass zwei Elemente A, deren entsprechende Zahlen nur durch das Vorzeichen unterschieden sind, als nicht verschieden anzusehen sind.

Die so definirte Gruppe, deren Grad für $p = 2$ durch (4) und für ein ungerades p durch (6) ausgedrückt ist, wollen wir die zum Körper $\mathfrak{E}$ gehörige Congruenzgruppe nennen und mit E bezeichnen.

Für die genauere Untersuchung dieser Gruppe ist es von Wichtigkeit, ein System erzeugender Substitutionen zu kennen. Stellen wir nach §. 64, (2) die Zahlen von $\mathfrak{E}$ in der Form dar:

$$\xi = x_0 + x_1 \varepsilon_1 + \cdots + x_{n-1} \varepsilon^{n-1}, \tag{7}$$

worin die x_i rationale, nach dem Modul p genommene Zahlen

bedeuten, so erhalten wir ein System erzeugender Substitutionen in der Form:

$$(8) \qquad A_0 = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad B_h = \begin{pmatrix} 1, & 0 \\ \varepsilon^h, & 1 \end{pmatrix}, \quad h = 0, 1, \ldots, n-1.$$

Um dies nachzuweisen, bemerken wir, dass

$$\begin{pmatrix} 1, & 0 \\ \gamma, & 1 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ \gamma', & 1 \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ \gamma + \gamma', & 1 \end{pmatrix}$$

ist; und durch wiederholte Anwendung hiervon, folgt, wenn

$$\gamma = c_0 + c_1 \varepsilon + \cdots + c_{n-1} \varepsilon^{n-1}$$

mit ganzen rationalen Coëfficienten c eine beliebige Zahl in $\mathfrak{E}$ ist,

$$(9) \qquad \begin{pmatrix} 1, & 0 \\ \gamma, & 1 \end{pmatrix} = B_0^{c_0} B_1^{c_1} \ldots B_{n-1}^{c_{n-1}}.$$

Ferner folgt durch Zusammensetzung mit A_0:

$$(10) \quad \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ \alpha, & 1 \end{pmatrix} = \begin{pmatrix} \alpha, & 1 \\ -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 0 \\ \delta, & 1 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

$$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ -\beta, & 1 \end{pmatrix} \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} = \begin{pmatrix} 1, & \beta \\ 0, & 1 \end{pmatrix}.$$

Daraus geht hervor, dass man aus den Elementen (8) alle Substitutionen von der Form

$$\begin{pmatrix} \alpha, & 1 \\ -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & \beta \\ 0, & 1 \end{pmatrix}, \quad \begin{pmatrix} 1, & 0 \\ \gamma, & 1 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

zusammensetzen kann, worin $\alpha, \beta, \gamma, \delta$ beliebige Zahlen in $\mathfrak{E}$ sind. Ferner ist

$$(11) \quad \begin{pmatrix} \alpha, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} 1, & \beta \\ 0, & 1 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ \gamma, & 1 \end{pmatrix} = \begin{pmatrix} \alpha + \gamma + \alpha\beta\gamma, & \alpha\beta + 1 \\ -\beta\gamma - 1, & -\beta \end{pmatrix}.$$

Nimmt man β von Null verschieden an, so kann man α und γ so wählen, dass $\alpha\beta + 1$, $-\beta\gamma - 1$ beliebige Zahlen werden, und nach (11) kann man also alle Substitutionen $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, worin δ von Null verschieden ist, aus A_0, B_h zusammensetzen. Die Beschränkung, dass δ von Null verschieden sei, kann aber nach der Formel

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & 0 \end{pmatrix} = \begin{pmatrix} -\beta, & \alpha \\ 0, & \gamma \end{pmatrix} \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$$

fallen gelassen werden.

Die Gruppe E enthält einen Theiler vom Index $p^n + 1$, der aus allen Substitutionen der Form

$$\begin{pmatrix} \alpha, & \beta \\ 0, & \delta \end{pmatrix}$$

besteht, worin β jede beliebige, α jede von Null verschiedene Zahl in $\mathfrak{E}$ bedeutet, und $\delta = \alpha^{-1}$ ist.

Diesem Theiler entspricht eine der Gruppe E isomorphe Permutationsgruppe von $p^n + 1$ Ziffern, die man so bilden kann:

Der lineare Ausdruck

$$(12) \qquad \eta = \frac{\alpha\xi + \beta}{\gamma\xi + \delta} \text{ oder } \xi = \frac{\delta\eta - \beta}{-\gamma\eta + \alpha}$$

giebt für jede Zahl ξ aus $\mathfrak{E}$ eine entsprechende Zahl η, ausgenommen, wenn $\gamma\xi + \delta = 0$ ist. Ebenso giebt es zu jedem η ein bestimmtes ξ, ausgenommen für $\gamma\eta - \alpha = 0$. Um diese Ausnahme zu beseitigen, genügt es, das System $\mathfrak{E}$ durch Hinzufügung eines Elementes, das wir „Unendlich" nennen und mit ∞ bezeichnen, zu erweitern. Mit diesem Zeichen wird nach den folgenden Regeln gerechnet, worin α irgend ein Element des erweiterten Systemes E bedeutet:

$$\begin{array}{lll}
\alpha + \infty = \alpha - \infty = \infty, & \text{ausser für} & \alpha = \infty \\
\alpha \,.\, \infty = \infty & \text{„ \quad „} & \alpha = 0 \\
\alpha : 0 = \infty & \text{„ \quad „} & \alpha = 0 \\
\alpha : \infty = 0 & \text{„ \quad „} & \alpha = \infty.
\end{array}$$

Dann führt das Ergebniss jeder Rechnung mit den vier Species immer zu einer bestimmten Zahl des Systems E und nur die Verbindungen $\infty \pm \infty$, $0 \,.\, \infty$, $0 : 0$, $\infty : \infty$ bleiben ohne Bedeutung.

Nach (12) entspricht dann der Zahl $\xi = -\delta : \gamma$ die Zahl $\eta = \infty$, und der Zahl $\xi = \infty$ die Zahl $\eta = \alpha : \gamma$, und jeder Substitution A in E entspricht eine bestimmte Permutation der $p^n + 1$ Elemente des erweiterten Systemes $\mathfrak{E}$. Man sieht leicht, dass nur die identische Substitution alle diese Elemente ungeändert lässt, und dass folglich auch zwei verschiedene Substitutionen aus E immer verschiedene Permutationen hervorrufen. Der Isomorphismus ist also einstufig.

§. 66.
Einfachheit der Gruppe E.

Die erste Frage bei einer eingehenderen Untersuchung der Gruppe E ist die nach einem etwa vorhandenen Normaltheiler. Es lässt sich beweisen, dass ein solcher Normaltheiler, von zwei ganz einfachen Ausnahmen abgesehen, nicht vorhanden ist.

Nehmen wir an, es sei G ein Normaltheiler von E, der wenigstens eine von der Identität verschiedene Substitution

$$A = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \tag{1}$$

enthält. Nach dem Begriffe des Normaltheilers ist dann, wenn T ein beliebiges Element in E ist,

$$T A T^{-1} \tag{2}$$

auch in G enthalten, und es ist zu zeigen, dass man auf diese Weise und durch Zusammensetzung solcher Substitutionen alle Elemente von E ableiten kann, woraus dann folgt, dass G mit E identisch sein muss. Es genügt aber dazu, das Vorkommen der erzeugenden Substitutionen A_0, B_h [§. 65, (8)] in G nachzuweisen.

Wir gehen dazu schrittweise vor.

1) In G kommt eine Substitution von der Form

$$\begin{pmatrix} 0, & \beta \\ \gamma, & \delta \end{pmatrix} \tag{3}$$

vor. Um dies zu zeigen, bilden wir nach (2):

$$\begin{pmatrix} \xi, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} 0, & -1 \\ 1, & \xi \end{pmatrix} = \begin{pmatrix} \beta\xi + \delta, & \beta\xi^2 + (\delta - \alpha)\xi - \gamma \\ -\beta, & -\beta\xi + \alpha \end{pmatrix}. \tag{4}$$

Wenn nun β von Null verschieden ist, so kann man ξ aus $\beta\xi + \delta = 0$ bestimmen und hat das Ziel erreicht. Ist aber $\beta = 0$, so ist nicht gleichzeitig $\gamma = 0$, $\delta - \alpha = 0$, weil sonst A die identische Substitution wäre; man kann daher ξ so annehmen, dass $(\delta - \alpha)\,\xi - \gamma$ von Null verschieden ist. Dann hat man durch (4) eine Substitution A in G gebildet, in der β nicht Null ist, und auf die man die Formel (4) nun nochmals anwenden kann, um α zu Null zu machen.

2) In G kommt eine Substitution von der Form

$$\begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix}$$

vor. Um dies nachzuweisen, bilden wir nach (2):

$$(5)\qquad \begin{pmatrix}\lambda, & \mu\\ \nu, & \varrho\end{pmatrix}\begin{pmatrix}0, & \beta\\ \gamma, & \delta\end{pmatrix}\begin{pmatrix}\varrho, & -\mu\\ -\nu, & \lambda\end{pmatrix} =$$

$$\begin{pmatrix}\mu\varrho\gamma - \lambda\nu\beta - \mu\nu\delta, & -\mu^2\gamma + \lambda^2\beta + \lambda\mu\delta\\ \varrho^2\gamma - \nu^2\beta - \varrho\nu\delta, & -\varrho\mu\gamma + \lambda\nu\beta + \lambda\varrho\delta\end{pmatrix},$$

und es ist also nur zu zeigen, dass man $\lambda, \mu, \nu, \varrho$ so bestimmen kann, dass die drei Gleichungen:

$$(6)\qquad \begin{aligned} \lambda\varrho - \mu\nu &= 1\\ \mu\varrho\gamma - \lambda\nu\beta - \mu\nu\delta &= 0\\ -\mu^2\gamma + \lambda^2\beta + \lambda\mu\delta &= 1\end{aligned}$$

befriedigt sind. Aus den beiden letzten Gleichungen folgt aber, wenn man sie zuerst mit μ, ϱ, dann mit λ, ν multiplicirt und jedesmal addirt, mit Benutzung der ersten Gleichung:

$$(7)\qquad \lambda\beta + \mu\delta = \varrho, \quad \mu\gamma = \nu,$$

und wenn man diese Werthe von ϱ, ν in die erste Gleichung (6) einsetzt:

$$(8)\qquad \lambda^2\beta + \lambda\mu\delta - \mu^2\gamma = 1.$$

Diese Gleichung kann aber immer befriedigt werden. Denn wegen $\beta\gamma = -1$ kann keine der beiden Zahlen β, γ verschwinden. Ist nun β ein Quadrat, so können wir $\mu = 0$ setzen und λ aus $\lambda^2\beta = 1$ bestimmen. Dies ist immer möglich bei $p = 2$. Ist aber p ungerade, so erhalten wir, wenn β ein Nichtquadrat ist, aus (8):

$$(2\lambda\beta + \delta\mu)^2 + \mu^2(4 - \delta^2) = 4\beta.$$

Ist nun zunächst $4 - \delta^2$ Nichtquadrat, so kann man μ aus $\mu^2(4 - \delta^2) = 4\beta$ und dann λ aus $2\lambda\beta + \delta\mu = 0$ bestimmen. Ist aber $4 - \delta^2$ Quadrat, so zerlege man 4β nach §. 64, 7. in die Summe aus zwei Quadraten $4\beta = \sigma^2 + \tau^2$ und bestimme μ und λ aus

$$\mu^2(4 - \delta^2) = \sigma^2, \quad 2\lambda\beta + \delta\mu = \tau.$$

Hat man so λ und μ ermittelt, so erhält man ϱ und ν aus (7), und dadurch sind die Gleichungen (6) thatsächlich befriedigt. Damit ist das Ziel erreicht.

3) Die Gruppe G enthält die Substitution

$$A_0 = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix},$$

mit alleiniger Ausnahme des Falles $n = 1$, $p = 2$. Zunächst haben wir in G die Substitutionen

$$\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & \xi\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix} = \begin{pmatrix}\xi, & 1\\ -1, & 0\end{pmatrix},$$

also auch

$$\begin{pmatrix}0, & 1\\ -1, & \xi\end{pmatrix}\begin{pmatrix}\xi, & 1\\ -1, & 0\end{pmatrix} = \begin{pmatrix}1, & 0\\ 2\xi, & 1\end{pmatrix},$$

und mithin

$$\begin{pmatrix}1, & 0\\ 2\xi, & 1\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & \xi\end{pmatrix} = \begin{pmatrix}0, & 1\\ -1, & 3\xi\end{pmatrix},$$

$$\begin{pmatrix}1, & 0\\ 2\xi, & 1\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & 3\xi\end{pmatrix} = \begin{pmatrix}0, & 1\\ -1, & 5\xi\end{pmatrix} \text{ u. s. f.,}$$

$$\begin{pmatrix}0, & 1\\ -1, & m\xi\end{pmatrix}$$

für jede ungerade ganze Zahl m; wenn also p ungerade ist, so können wir $m = p$ annehmen und erhalten A_0. Ist aber $p = 2$, so haben wir, wenn wir mit ϱ eine noch zu bestimmende Zahl in $\mathfrak{E}$ bezeichnen, folgende Substitutionen in G:

$$\begin{pmatrix}0, & \varrho\\ -\varrho^{-1}, & 0\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & \xi\end{pmatrix}\begin{pmatrix}0, & -\varrho\\ \varrho^{-1}, & 0\end{pmatrix} = \begin{pmatrix}\xi, & \varrho^2\\ -\varrho^{-2}, & 0\end{pmatrix}.$$

Da hier nun jede Zahl ein Quadrat ist, so kann man ϱ^2 auch durch ϱ ersetzen, und findet also, dass in G die Substitution

$$\begin{pmatrix}\xi, & \varrho\\ -\varrho^{-1}, & 0\end{pmatrix}$$

für jedes beliebige von Null verschiedene ϱ, und folglich auch die entgegengesetzte Substitution

$$\begin{pmatrix}0, & -\varrho\\ \varrho^{-1}, & \xi\end{pmatrix}$$

vorkommen muss. Bedeuten also ϱ, σ zwei von Null verschiedene Zahlen, so haben wir in G auch

$$(9) \qquad \begin{pmatrix}0, & \varrho^{-1}\sigma^{-1}\\ -\varrho\sigma, & \xi\end{pmatrix}\begin{pmatrix}\xi, & \sigma^{-1}\\ -\sigma, & 0\end{pmatrix}\begin{pmatrix}0, & \varrho\\ -\varrho^{-1}, & \xi\end{pmatrix}$$
$$= \begin{pmatrix}0, & 1\\ -1, & \xi\varrho\,(1+\sigma+\sigma\varrho)\end{pmatrix}.$$

Wenn nun n grösser als 1 ist, so kann man ϱ und $1 + \varrho$ von Null verschieden annehmen und dann $\sigma = -1 : (1 + \varrho)$ setzen, wodurch die Substitution (9) in A_0 übergeht.

Ist aber $n = 1$ und $p = 2$, so tritt der erste Ausnahmefall ein; denn dann ist immer eine der beiden Zahlen ϱ und $1 + \varrho$ gleich Null. Dieser Fall führt auf eine Gruppe 6ten Grades

$$E = \begin{pmatrix}1, 0\\0, 1\end{pmatrix}, \begin{pmatrix}1, 0\\1, 1\end{pmatrix}, \begin{pmatrix}0, 1\\1, 1\end{pmatrix}, \begin{pmatrix}1, 1\\1, 0\end{pmatrix}, \begin{pmatrix}1, 1\\0, 1\end{pmatrix}, \begin{pmatrix}0, 1\\1, 0\end{pmatrix},$$

in der ein Normaltheiler 3ten Grades enthalten ist:

$$G = \begin{pmatrix}1, 0\\0, 1\end{pmatrix}, \begin{pmatrix}0, 1\\1, 1\end{pmatrix}, \begin{pmatrix}1, 1\\1, 0\end{pmatrix}.$$

Von diesem Ausnahmefalle sehen wir jetzt ab. Wir haben dann weiter:

4) Die Gruppe G enthält jede Substitution von der Form

$$(10) \qquad \begin{pmatrix}1, 0\\\xi, 1\end{pmatrix},$$

worin ξ eine beliebige Zahl in $\mathfrak{E}$ ist, ausgenommen in dem Falle $n = 1$, $p = 3$.

Denn nach 3) enthält G die Substitution

$$\begin{pmatrix}0, & \varrho\\-\varrho^{-1}, & 0\end{pmatrix}\begin{pmatrix}0, & 1\\-1, & 0\end{pmatrix}\begin{pmatrix}0, & -\varrho\\\varrho^{-1}, & 0\end{pmatrix}\begin{pmatrix}0, & 1\\-1, & 0\end{pmatrix} = \begin{pmatrix}\varrho^2, & 0\\0, & \varrho^{-2}\end{pmatrix},$$

wenn ϱ eine beliebige von Null verschiedene Zahl in $\mathfrak{E}$ ist. Daraus folgt, dass auch

$$(11) \qquad \begin{pmatrix}1, & 0\\-\lambda, & 1\end{pmatrix}\begin{pmatrix}\varrho^{-2}, & 0\\0, & \varrho^2\end{pmatrix}\begin{pmatrix}1, & 0\\\lambda, & 1\end{pmatrix}\begin{pmatrix}\varrho^2, & 0\\0, & \varrho^{-2}\end{pmatrix} = \begin{pmatrix}1, & 0\\\lambda(\varrho^4 - 1), & 1\end{pmatrix}$$

für jedes beliebige λ in G vorkommt. Kann man nun ϱ von Null verschieden so annehmen, dass $\varrho^4 - 1$ nicht verschwindet, so kann man für jedes ξ die Zahl λ aus $\lambda(\varrho^4 - 1) = \xi$ bestimmen, und erhält also aus (11) jede Substitution der Form (10). Um die Möglichkeit hiervon zu beurtheilen, nehmen wir eine primitive Wurzel γ von $\mathfrak{E}$ an und setzen $\varrho = \gamma^h$.

Kann man den Exponenten h so annehmen, dass $4h$ nicht durch $p^n - 1$ theilbar ist, so genügt ϱ unserer Forderung. Dies ist immer möglich, wenn $p = 2$, $n > 1$ ist, und wenn $p^n - 1 > 4$ ist, und es bleiben also nur die beiden Fälle $n = 1$, $p = 3$ und $n = 1$, $p = 5$ noch zweifelhaft.

In dem Falle $n = 1$, $p = 5$ haben wir aber in G nach (2) und 3) die Substitution

$$\begin{pmatrix}1, & 1\\ 2, & -2\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}-2, & -1\\ -2, & 1\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix} = \begin{pmatrix}-2, & 0\\ 0, & 2\end{pmatrix},$$

und folglich auch

$$(12) \quad \begin{pmatrix}1, & 0\\ -\xi, & 1\end{pmatrix}\begin{pmatrix}-2, & 0\\ 0, & 2\end{pmatrix}\begin{pmatrix}1, & 0\\ \xi, & 1\end{pmatrix}\begin{pmatrix}2, & 0\\ 0, & -2\end{pmatrix} = \begin{pmatrix}1, & 0\\ -2\xi, & 1\end{pmatrix},$$

also, da ξ und folglich auch -2ξ beliebig ist, wieder die Substitutionen (10) und damit also alle Erzeugenden der Gruppe E, und also ist in allen diesen Fällen G mit E identisch und folglich die Gruppe E einfach.

Der Fall $n = 1$, $p = 3$ bietet aber die zweite wirkliche Ausnahme. In diesem Falle ist die Gruppe E vom 12ten Grade und sie hat den Normaltheiler 4ten Grades

$$G = \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}, \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}, \begin{pmatrix}-1, & 1\\ 1, & 1\end{pmatrix}, \begin{pmatrix}1, & 1\\ 1, & -1\end{pmatrix}.$$

Um sich davon zu überzeugen, braucht man nur die beiden Nebengruppen:

$$\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix} G = \begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}, \begin{pmatrix}0, & 1\\ -1, & 1\end{pmatrix}, \begin{pmatrix}-1, & 1\\ 0, & -1\end{pmatrix}, \begin{pmatrix}1, & 1\\ -1, & 0\end{pmatrix}$$

$$\begin{pmatrix}1, & 0\\ -1, & 1\end{pmatrix} G = \begin{pmatrix}1, & 0\\ -1, & 1\end{pmatrix}, \begin{pmatrix}0, & 1\\ -1, & -1\end{pmatrix}, \begin{pmatrix}-1, & 1\\ -1, & 0\end{pmatrix}, \begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix}$$

mit $G\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}$, $G\begin{pmatrix}1, & 0\\ -1, & 1\end{pmatrix}$ zu vergleichen.

Damit ist also allgemein bewiesen, dass, von den beiden Fällen $n = 1$, $p = 2$ und $n = 1$, $p = 3$ abgesehen, die Gruppe E einfach ist. Für die ersten Fälle erhält man für die Grade g dieser einfachen Gruppen:

$n = 1$,	$p = 5$,	$g = 60$	$n = 2$,	$p = 2$,	$g = 60$
	$p = 7$,	$g = 168$		$p = 3$,	$g = 360$
	$p = 11$,	$g = 660$		$p = 5$,	$g = 7800$
	$p = 13$,	$g = 1092$	$n = 3$,	$p = 2$,	$g = 504$
				$p = 3$,	$g = 9828$
			$n = 4$,	$p = 2$,	$g = 4080$[1].

[1]) Siehe Bulletin of the New York math. Society. October 1893. In dem Berichte über den mathematischen Congress in Chicago finden sich zwei Notizen über diese Gruppen von Cole und Moore.

§. 67.

Congruenzkörper zweiten Grades.

In jedem Congruenzkörper $\mathfrak{E}_{n,p}$ für den Modul p vom n^{ten} Grade ist der Congruenzkörper ersten Grades $\mathfrak{E}_{1,p}$, der aus den nach dem Modul p genommenen rationalen Zahlen besteht, als Theiler enthalten. Daher ist auch in der Gruppe der linearen Substitutionen $E_{n,p}$ eine Gruppe als Theiler enthalten, die aus allen Substitutionen der Form

$$(1) \qquad A = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}, \quad ab - cd = 1$$

besteht, worin a, b, c, d nach dem Modul p genommene ganze rationale Zahlen sind.

Diese Gruppe, die als die Gruppe der Modulargleichungen in der Theorie der elliptischen Functionen auftritt[1]), ist das eigentliche Ziel unserer Betrachtungen. Es bietet aber für die Untersuchung dieser Gruppe, und besonders für die Aufsuchung ihrer Theiler, den grössten Vortheil, diese Gruppe nicht selbstständig für sich zu betrachten, sondern als Theiler einer Gruppe $E_{2,p}$. Bezeichnen wir nämlich mit N irgend einen feststehenden quadratischen Nichtrest von p, so ist, wie schon oben bemerkt, $t^2 - N$ nach dem Modul p irreducibel, und wir erhalten einen Congruenzkörper 2ten Grades, wenn wir eine Galois'sche imaginäre Zahl durch die Gleichung

$$(2) \qquad \varepsilon^2 = N$$

einführen.

Es soll der Deutlichkeit wegen für die nächsten Betrachtungen festgesetzt sein, dass die kleinen lateinischen Buchstaben ganze rationale Zahlen (nach dem Modul p genommen), die wir hier auch reelle Zahlen nennen, die griechischen Buchstaben Zahlen des Körpers $\mathfrak{E}_{2,p}$ bedeuten sollen.

Dieser Körper $\mathfrak{E}_{2,p}$ hat die für uns sehr wichtige Eigenschaft, dass in ihm alle reellen Zahlen Quadrate sind.

Wenn nämlich a quadratischer Rest von p ist, so können wir $a = x^2$ setzen, und wenn b quadratischer Nichtrest ist, so kann $x^2 = bN$ befriedigt werden, also $b = (x\varepsilon^{-1})^2$.

---

1) Man vergleiche des Verfassers Buch: „Elliptische Functionen und algebraische Zahlen". Braunschweig 1891.

Eine Zahl von der Form $a\varepsilon$ soll eine **rein imaginäre Zahl** heissen, zwei Zahlen der Form $a + b\varepsilon$, $a - b\varepsilon$ **conjugirt imaginäre Zahlen**. Die Uebertragung dieser Bezeichnungen aus der Theorie der gewöhnlichen complexen Zahlen auf die Zahlen des Körpers $\mathfrak{E}_{2,p}$ rechtfertigt sich durch die Uebereinstimmung der Rechenregeln und kann zu keinem Missverständniss führen, da in diesen Betrachtungen von den gewöhnlichen complexen Zahlen nicht die Rede ist.

Weil immer, wenn N ein quadratischer Nichtrest ist, $N^{1/2(p-1)} = -1$ ist, so folgt aus (2):

$$(3) \qquad \varepsilon^p = -\varepsilon.$$

Wendet man den binomischen Satz auf die p^{te} Potenz des Binoms $\alpha = a + b\varepsilon$ an, und beachtet, dass alle Binomialcoëfficienten, mit Ausnahme des ersten und des letzten, durch p theilbar, also hier $= 0$ sind, dass ferner nach dem Fermat'schen Satze $a^p = a$, $b^p = b$ ist, so ergiebt sich nach (3):

$$(4) \qquad \alpha = a + b\varepsilon, \quad \alpha^p = a - b\varepsilon,$$

und folglich durch Multiplication:

$$(5) \qquad \alpha^{p+1} = a^2 - Nb^2,$$

woraus folgt, dass α^{p+1} immer eine reelle Zahl ist.

Ist γ eine primitive Wurzel des Körpers $\mathfrak{E}_{2,p}$ [§. 64, (8)], so ist γ^r dann und nur dann reell, wenn r durch $p+1$ theilbar ist, und γ^{p+1} ist eine primitive Wurzel der Primzahl p im gewöhnlichen Sinne.

Die nothwendige und hinreichende Bedingung dafür, dass eine Zahl α in $\mathfrak{E}_{2,p}$ reell ist, besteht in der Gleichung $\alpha^p = \alpha$.

Jede reelle Zahl ist als $(p+1)^{te}$ Potenz einer Zahl in $\mathfrak{E}_{2,p}$ darstellbar.

Denn dass γ^r reell ist, wenn r durch $p+1$ theilbar ist, folgt aus (5). Dass es aber nicht anders reell sein kann, ergiebt sich daraus, dass nach dem Fermat'schen Satze jede reelle von Null verschiedene Zahl der Bedingung $a^{p-1} = 1$ genügt, dass also, wenn γ^r reell ist, $\gamma^{r(p-1)} = 1$ sein muss, und es muss daher $r(p-1)$ durch p^2-1 und folglich r durch $p+1$ theilbar sein. Da ferner $\gamma^{r(p+1)}$ nur dann $= 1$ ist, wenn r durch $p-1$ theilbar ist, so ist γ^{p+1} primitive Wurzel von p.

Auch der Begriff der Einheitswurzeln lässt sich auf die Zahlen des Körpers $\mathfrak{E}_{2,p}$ übertragen.

Ist m ein Theiler von $p^2 - 1$, und

$$\varrho = \gamma^{\frac{p^2-1}{m}},$$

so ist $\varrho^m = 1$ und es giebt keine niedrigere als die m^{te} Potenz von ϱ, die gleich 1 wird. Daher nennen wir ϱ eine primitive m^{te} Einheitswurzel (in $\mathfrak{C}_{2,p}$). Alle anderen m^{ten} Einheitswurzeln sind dann Potenzen ϱ^s von ϱ und unter diesen sind die und nur die primitiv, bei denen s relativ prim zu m ist.

Dies folgt daraus, dass jede von Null verschiedene Zahl ξ in der Form $\xi = \gamma^r$ darstellbar ist, und dass $\xi^m = \gamma^{rm}$ dann und nur dann $= 1$ ist, wenn rm durch $p^2 - 1$ theilbar ist.

Jede von Null verschiedene Zahl in $\mathfrak{C}_{2,p}$ ist eine Einheitswurzel vom Grade $p^2 - 1$.

§. 68.

Die reelle lineare Congruenzgruppe L_p.

Wir gehen nun, mit diesen Hülfsmitteln ausgestattet, an die Untersuchung der reellen Congruenzgruppe L_p, die aus allen Substitutionen der Form

$$A = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$$

besteht, worin a, b, c, d reelle, nach dem Modul p genommene ganze Zahlen sind, die der Bedingung $ad - bc \equiv 1$ genügen. Die Gruppe L_p ist nach der früheren Bezeichnung mit $E_{1,p}$ zu bezeichnen, und ihr Grad ist, wenn wir den Fall $p = 2$ ausschliessen:

$$\frac{p\,(p^2 - 1)}{2}.$$

Sind A, U irgend zwei Elemente aus einer Gruppe, so haben wir schon früher

$$U^{-1} A\, U = A'$$

das durch U aus A transformirte Element genannt. $A'^2, A'^3, \ldots$ sind transformirt aus $A^2, A^3, \ldots$, woraus folgt, dass alle aus einander durch Transformation gewonnenen Elemente denselben Grad haben. Entnehmen wir die Elemente A aus irgend einer Gruppe G, so bilden die transformirten Elemente eine mit G isomorphe Gruppe

$$U^{-1} G\, U = G',$$

die wir die transformirte Gruppe von G nennen.

Es möge nun A irgend ein Element der Gruppe L_p sein, und $U = \begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$ ein Element aus $E_{2,p}$. Wir wollen aus A durch Transformation mit U eine gewisse Normalform ableiten.

Es soll zunächst versucht werden, A in die Normalform

(1) $$S = \begin{pmatrix} \sigma, & 0 \\ 0, & \sigma^{-1} \end{pmatrix}$$

zu transformiren. Aus der Gleichung

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix} = \begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix} \begin{pmatrix} \sigma, & 0 \\ 0, & \sigma^{-1} \end{pmatrix}$$

erhält man

(2) $$\begin{aligned} &(a - \sigma)\, \lambda + b\, \nu = 0, \quad (a - \sigma^{-1})\, \mu + b\, \varrho = 0, \\ &c\, \lambda + (d - \sigma)\, \nu = 0, \quad c\, \mu + (d - \sigma^{-1})\, \varrho = 0, \end{aligned}$$

und daraus ergiebt sich, dass σ und σ^{-1} die Wurzeln der quadratischen Gleichung

$$(a - \sigma)\,(d - \sigma) - b\, c = 0$$

oder

(3) $$\sigma^2 - \sigma\,(a + d) + 1 = 0$$

sein müssen. Hat man σ und σ^{-1} hieraus bestimmt, so findet man aus (2) die Verhältnisse $\lambda : \nu$ und $\mu : \varrho$. Die Grössen $\lambda, \mu, \nu, \varrho$ selbst sind dann noch so zu bestimmen, dass $\lambda\varrho - \mu\nu = 1$ wird. Dies ist immer möglich, wenn die aus (2) bestimmten Werthe nicht die Gleichung $\lambda\varrho = \mu\nu$ erfüllen. Sind b und c beide $= 0$, so hat A schon die Form (1). Ist aber eine der beiden Zahlen b, c, etwa b, von Null verschieden, so ergiebt sich aus (2):

(4) $$\frac{\nu}{\lambda} = -\frac{(a - \sigma)}{b}, \quad \frac{\varrho}{\mu} = -\frac{(a - \sigma^{-1})}{b},$$

und es kann nur dann $\lambda\varrho = \mu\nu$ oder $\nu : \lambda = \varrho : \mu$ sein, wenn $\sigma = \sigma^{-1}$, also $\sigma = \pm 1$ ist, d. h. nach (3), wenn $a + d = \pm 2$ ist.

Die Gleichung (3) ist aber im Körper $\mathfrak{E}_{2,p}$ immer lösbar, weil jede reelle Zahl in diesem Körper ein Quadrat ist, und ergiebt

(5) $$\begin{aligned} \sigma &= \frac{a + d}{2} + \sqrt{\left(\frac{a + d}{2}\right)^2 - 1} \\ \sigma^{-1} &= \frac{a + d}{2} - \sqrt{\left(\frac{a + d}{2}\right)^2 - 1} \end{aligned}$$

Wir kommen also zu dem ersten Resultate:

1. Eine Substitution A ist immer auf die Normalform S transformirbar, wenn $a+d$ nicht $=\pm 2$ ist. σ ist reell oder imaginär, je nachdem $(a+d)^2-4$ quadratischer Rest oder Nichtrest von p ist.

In dem noch übrigen Falle, wo $a+d=\pm 2$ ist, lässt sich die Normalform S nicht herstellen; dagegen können wir A in diesem Falle auf eine andere Normalform, nämlich

$$T=\begin{pmatrix}1, & t\\ 0, & 1\end{pmatrix} \tag{6}$$

bringen, in der t reell ist.

Um dies zu beweisen, können wir zunächst

$$a+d=+2 \tag{7}$$

annehmen, weil der andere Fall $a+d=-2$ durch Aenderung aller Vorzeichen von a, b, c, d auf diesen zurückgeführt wird.

Aus (7) aber folgt noch

$$a-1=-(d-1),\quad (a-1)(d-1)=bc. \tag{8}$$

Wenn also zunächst b oder $c=0$ ist, so ist $a=d=1$ und wir haben entweder

$$A=\begin{pmatrix}1, & b\\ 0, & 1\end{pmatrix},$$

was schon die Normalform T hat, oder

$$A=\begin{pmatrix}1, & 0\\ c, & 1\end{pmatrix}=\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}1, & -c\\ 0, & 1\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix},$$

so dass $\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix} A \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$ die Normalform T hat. Sind aber b und c von Null verschieden, so erhalten wir aus (8) die Transformation

$$\begin{pmatrix}(d-1)\,b^{-1}, & 0,\\ -1, & (a-1)\,c^{-1}\end{pmatrix}\begin{pmatrix}a, & b\\ c, & d\end{pmatrix}\begin{pmatrix}(a-1)\,c^{-1}, & 0,\\ 1, & (d-1)\,b^{-1}\end{pmatrix}$$
$$=\begin{pmatrix}1, & -c\\ 0, & 1\end{pmatrix},$$

was die Form T hat. Damit ist also bewiesen:

2. Eine Substitution A, in der $a+d=\pm 2$ ist, kann immer durch Transformation auf die Normalform T gebracht werden.

Hiernach lassen sich leicht die Grade der Elemente unserer Gruppe bestimmen. Wir haben dabei drei Fälle zu unterscheiden.

I. $a + d = \pm 2$. Jede Substitution dieser Art lässt sich in die Normalform T transformiren. Es ist aber für jeden Exponenten r

$$T^r = \begin{pmatrix} 1, & rt \\ 0, & 1 \end{pmatrix},$$

und folglich ist der Grad dieser Substitution p, ausser wenn $t = 0$, also T die identische Substitution ist.

Die Anzahl der Elemente dieser Art ist leicht zu bestimmen. Nehmen wir zunächst $c = 0$, so können wir b beliebig wählen und für a, d erhalten wir aus $a + d = \pm 2$, $ad = 1$ die beiden Bestimmungen $a = d = \pm 1$. Dies giebt $2p$ Formen, die identische Substitution eingeschlossen. Nehmen wir sodann a und c beliebig, jedoch c von Null verschieden, was $p(p-1)$ Möglichkeiten giebt, so folgt aus $ad - bc = 1$

$$b = -c^{-1} + adc^{-1},$$

und zu jedem a kann d auf zwei Arten bestimmt werden. Die Gesammtzahl $2p^2$, die wir so erhalten, ist noch zu halbiren, weil hier die Substitutionen als zwei verschiedene auftreten, in denen alle Zeichen entgegengesetzt sind; und wir erhalten also p^2 Substitutionen dieser Art (die identische eingeschlossen).

II. $(a + d)^2 - 4$ quadratischer Rest von p. Eine solche Substitution lässt sich in die Normalform S transformiren mit reellem σ.

Verstehen wir unter γ eine primitive Wurzel des Körpers $\mathfrak{E}_{2,p}$, so ist

$$\gamma^{\frac{p^2-1}{2}} = -1,$$

und wir können r so bestimmen, dass

$$\sigma = \gamma^{r(p+1)}, \quad \sigma^{\frac{p-1}{2}} = (-1)^r$$

wird (§. 67). Nach (5) erhalten wir dann

$$(9) \qquad a + d = \gamma^{r(p+1)} + \gamma^{-r(p+1)},$$

und weil nach (5) die beiden Werthe σ, σ^{-1}, von der Reihenfolge abgesehen, durch $a + d$ bestimmt sind, so werden zwei Werthe des Ausdrucks (9) nur dann einander gleich oder entgegengesetzt, wenn die entsprechenden Werthe, mit positivem oder

negativem Zeichen genommen, von r nach dem Modul $\frac{1}{2}(p-1)$ congruent sind. Man erhält daher alle von einander und von ± 2 verschiedenen Werthe dieses Ausdruckes, wenn man

$$(10) \qquad r = 1, 2, \ldots \frac{p-3}{2}$$

setzt. Da hier für jeden Exponenten k

$$S^k = \begin{pmatrix} \sigma^k, & 0 \\ 0, & \sigma^{-k} \end{pmatrix}$$

ist, so ist der Grad von S, und also auch von jeder Substitution der II^ten^ Art entweder $\frac{1}{2}(p-1)$ oder ein Theiler davon, je nachdem r relativ prim zu $\frac{1}{2}(p-1)$ ist oder nicht.

Um die Anzahl dieser Substitutionen zu bestimmen, verfahren wir wie oben. Ist zunächst $c = 0$, so ergiebt sich

$$a = \gamma^{\pm r(p+1)}, \quad d = \gamma^{\mp r(p+1)},$$

und b kann p Werthe haben. Die Zahl r hat die Werthe (10), und also ergeben sich hiernach $p(p-3)$ Substitutionen. Ist dann c von Null verschieden, so ist $p(p-1)$ die Anzahl der verschiedenen Annahmen über a, c. Ist a angenommen, so können wir d aus (9) bestimmen und

$$b = -c^{-1} + adc^{-1},$$

setzen, woraus wir $\frac{1}{2}p(p-1)(p-3)$ Bestimmungen erhalten, also mit den für $c = 0$ gezählten zusammen $\frac{1}{2}p(p-3)(p+1)$. Auch diese Zahl ist noch zu halbiren, so dass wir

$$\frac{1}{4}p(p-3)(p+1)$$

Substitutionen der II^ten^ Art erhalten.

III. $(a+d)^2 - 4$ quadratischer Nichtrest von p. In diesem Falle ist σ nicht reell, aber mit seinem reciproken Werth conjugirt. Also ist nach §. 67, (4) $\sigma^p = \sigma^{-1}$, und folglich

$$\sigma^{\frac{p+1}{2}} = \pm 1.$$

Daraus ergiebt sich, dass der Grad einer solchen Substitution $\frac{1}{2}(p+1)$ oder ein Theiler dieser Zahl ist.

In diesem dritten Falle setzen wir

$$(11) \qquad \sigma = \gamma^{r(p-1)}, \quad a + d = \gamma^{r(p-1)} + \gamma^{-r(p-1)}$$
$$r = 1, 2, \ldots, \tfrac{1}{2}(p-1).$$

Hier kann der Fall $c = 0$ oder $b = 0$ nicht vorkommen, weil sich aus $ad = 1$ ergeben würde, dass $a = \sigma^{\pm 1}$, $d = \sigma^{\mp 1}$

sein müsste, und es würden a und d nicht reell ausfallen. Also nehmen wir für a und c, wie oben, die $p(p-1)$ verschiedenen Werthsysteme, und erhalten aus (11) für jedes von ihnen $\frac{1}{2}(p-1)$ Bestimmungen von b und d; auch diese Zahl ist zu halbiren und es ergeben sich

$$\tfrac{1}{4}\, p\,(p-1)\,(p-1)$$

Substitutionen der III[ten] Art. Die Gesammtzahl aller Substitutionen der Gruppe L_p ist hiernach, wie es sein muss,

$$p^2 + \tfrac{1}{4} p (p-3)(p+1) + \tfrac{1}{4} p (p-1)^2 = \tfrac{1}{2} p (p^2 - 1).$$

§. 69.

Imaginäre Form der Gruppe L_p.

Die Substitutionen der beiden ersten Arten der Gruppe L_p haben die Eigenschaft, dass die ihnen entsprechende Normalform T oder S gleichfalls in L_p enthalten ist, und dass man sie in diese Normalformen transformiren kann durch **reelle** Substitutionen, d. h. durch Substitutionen, die selbst in L_p vorkommen. Beides trifft bei den Substitutionen der dritten Art nicht zu.

Man kann aber, wie wir jetzt beweisen werden, die ganze Gruppe L_p in eine andere Gruppe Λ_p so transformiren, dass Λ_p ein mit L_p **isomorpher Theiler der Gruppe** $E_{2,p}$ ist, dass die Normalformen der Transformationen dritter Art in Λ_p enthalten sind und dass jede Substitution dritter Art in Λ_p in die Normalform transformirt werden kann durch Substitutionen von Λ_p selbst.

Um eine solche Transformation von L_p zu finden, betrachten wir die Substitution

(1) $$S = \begin{pmatrix} \sigma, & 0 \\ 0, & \sigma^{-1} \end{pmatrix}$$

unter der Voraussetzung, dass σ und σ^{-1} conjugirt imaginär sind, und suchen die Substitution

(2) $$R = \begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$$

so zu bestimmen, dass

(3) $$R\,S\,R^{-1}$$

reell wird. Es ergiebt sich aber nach (1) und (2)

$$RSR^{-1} = \begin{pmatrix} \lambda\varrho\sigma - \mu\nu\sigma^{-1}, & -\lambda\mu(\sigma-\sigma^{-1}) \\ \varrho\nu(\sigma-\sigma^{-1}), & -\mu\nu\sigma + \varrho\lambda\sigma^{-1} \end{pmatrix},$$

und dies wird reell, wenn $\lambda\mu$ und $\varrho\nu$ rein imaginär, $\lambda\varrho$ und $-\mu\nu$ conjugirt imaginär sind. Diesen Bedingungen kann man auf mehrfache Art genügen: am einfachsten wohl, und zwar zugleich so, dass die Determinante von $R = 1$ wird, wenn man

(4) $$R = \begin{pmatrix} \frac{1}{2}, & -\frac{1}{2}\varepsilon^{-1} \\ \varepsilon, & 1 \end{pmatrix}$$

setzt. Ist andererseits

$$A = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$$

eine beliebige reelle Substitution aus L_p, so ergiebt sich nach (4) wegen $\varepsilon^2 = N$:

$$\mathsf{A} = R^{-1}AR =$$

(5) $$\begin{pmatrix} \frac{a+d}{2} + b\varepsilon + \frac{c}{4}\varepsilon^{-1}, & -\frac{a-d}{2}\varepsilon^{-1} + b - \frac{c}{4}N^{-1} \\ -N\left(\frac{a-d}{2}\varepsilon^{-1} + b - \frac{c}{4}N^{-1}\right), & \frac{a+d}{2} - b\varepsilon - \frac{c}{4}\varepsilon^{-1} \end{pmatrix},$$

wofür wir auch

(6) $$\mathsf{A} = \begin{pmatrix} \alpha, & \beta \\ -N\beta', & \alpha' \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ -N\beta^p, & \alpha^p \end{pmatrix}, \quad \alpha\alpha' + N\beta\beta' = 1$$

setzen, worin α, α' und β, β' zwei conjugirt imaginäre Paare sind, so dass nach §. 65, (4) $\alpha' = \alpha^p$, $\beta' = \beta^p$ gesetzt werden kann.

Wenn wir umgekehrt irgend eine Substitution A von der Form (6) nehmen, so ergiebt sich

$$A = R\mathsf{A}R^{-1} =$$

(7) $$\begin{pmatrix} \frac{\alpha+\alpha'}{2} + \varepsilon\frac{\beta'-\beta}{2}, & \frac{\beta+\beta'}{4} + \varepsilon^{-1}\frac{\alpha-\alpha'}{4} \\ -N(\beta+\beta') + \varepsilon(\alpha-\alpha'), & \frac{\alpha+\alpha'}{2} - \varepsilon\frac{\beta'-\beta}{2} \end{pmatrix}$$

als eine reelle Substitution aus L_p.

Daraus geht hervor, dass, wenn A die ganze Gruppe L_p durchläuft, die durch (5) und (6) bestimmte Substitution A eine mit L_p isomorphe Gruppe durchläuft, die wir mit A_p bezeichnen.

In der Gruppe A_p ist die Normalform S für die Substitutionen dritter Art enthalten.

Nehmen wir nun eine Substitution A von der dritten Art in der Gruppe A_p an, so können wir sie, wie jetzt noch nachgewiesen werden soll, durch Transformation mit einer Substitution U, die selbst der Gruppe A_p angehört, in die Normalform transformiren. Denn setzen wir

$$(8) \qquad A = \begin{pmatrix} \alpha, & \beta \\ -N\beta', & \alpha' \end{pmatrix}, \qquad U = \begin{pmatrix} \lambda, & \mu \\ -N\mu', & \lambda' \end{pmatrix},$$

$$(9) \qquad \alpha\alpha' + N\beta\beta' = 1, \qquad \lambda\lambda' + N\mu\mu' = 1,$$

worin λ, λ' und μ, μ' conjugirte Paare sind, so erhalten die Gleichungen (3), (4), §. 68 die Form:

$$(10) \quad (\sigma - \alpha)(\sigma - \alpha') + N\beta\beta' = \sigma^2 - \sigma(\alpha + \alpha') + 1 = 0,$$

$$(11) \qquad N\frac{\mu'}{\lambda} = \frac{\alpha - \sigma}{\beta}, \qquad \frac{\lambda'}{\mu} = -\frac{\alpha - \sigma^{-1}}{\beta},$$

und die Gleichung (10) muss, da A von der dritten Art sein soll, zwei zu einander reciproke, conjugirt imaginäre Wurzeln haben.

Aus der zweiten Gleichung (11) folgt aber durch Uebergang zu den conjugirt imaginären Zahlen

$$\frac{\lambda}{\mu'} = -\frac{\alpha' - \sigma}{\beta'},$$

und dies ist nach (10) eine Folge der ersten Gleichung (11). Setzen wir also

$$N\mu' = \varkappa(\alpha - \sigma), \qquad N\mu = \varkappa'(\alpha' - \sigma^{-1})$$
$$\lambda = \varkappa\beta, \qquad \lambda' = \varkappa'\beta',$$

worin $\varkappa, \varkappa'$ zwei conjugirt imaginäre Zahlen sind, so sind die Gleichungen (11) befriedigt, und man kann dann $\varkappa\varkappa'$ noch so bestimmen, dass $\lambda\lambda' + N\mu\mu' = 1$ wird.

Daraus ergiebt sich noch ein wichtiges Resultat. Bezeichnen wir mit γ eine primitive Wurzel des Körpers $\mathfrak{C}_{2,p}$, so können wir für die Substitutionen der Normalform für die zweite und dritte Art die Ausdrücke annehmen (§. 68):

$$S_2^r = \begin{pmatrix} \gamma^{(p+1)r}, & 0 \\ 0, & \gamma^{-(p+1)r} \end{pmatrix}, \qquad S_3^r = \begin{pmatrix} \gamma^{(p-1)r}, & 0 \\ 0, & \gamma^{-(p-1)r} \end{pmatrix}.$$

Ist nun A eine Substitution zweiter Art aus L_p und A eine

Substitution dritter Art aus $\varDelta_p$, so können wir die Substitutionen U, V aus L_p oder aus $\varDelta_p$ so bestimmen, dass

$$A = U S_2^r U^{-1}, \qquad A = V S_3^r V^{-1}.$$

Setzen wir also, dem Werth $r = 1$ entsprechend,

$$A_1 = U S_2 U^{-1}, \qquad A_1 = V S_3 V^{-1},$$

so ergiebt sich

$$A = A_1^r, \qquad A = A_1^r,$$

und A_1 kommt in L_p, A_1 in $\varDelta_p$ vor.

Ist ferner B eine Substitution erster Art aus L_p, so kann man wieder, wenn man

$$T_1 = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}$$

setzt, U aus L_p so bestimmen, dass

$$B = U T_1^r U^{-1} = B_1^r$$

wird. Hieraus ergiebt sich der Satz:

Man kann in der Gruppe L_p (oder $\varDelta_p$) die Substitutionen der ersten, zweiten und dritten Art mit Hinzuziehung der Identität in Cyklen von p, $\frac{p-1}{2}$, $\frac{p+1}{2}$ Gliedern anordnen.

Zwei solche Cyklen können ausser dem Einheitselemente kein Glied gemein haben.

Dies ist zunächst evident bei den Substitutionen der ersten Art, deren Grad gleich p ist; denn bei diesen lässt sich der ganze Cyklus durch Potenzirung aus einem beliebigen von der Einheit verschiedenen Elemente ableiten.

Wenn aber in zwei Cyklen der zweiten oder dritten Art ein gemeinsames Element vorkommt, so kann die Gruppe so transformirt werden, dass die beiden Cyklen die Gestalt bekommen:

$$(12) \qquad \begin{array}{llll} 1, & U S U^{-1}, & U S^2 U^{-1}, & \ldots \\ 1, & S, & S^2, & \ldots, \end{array}$$

worin $S = \begin{pmatrix} \sigma, & 0 \\ 0, & \sigma^{-1} \end{pmatrix}$ die Normalform hat.

Ist nun für irgend zwei von Null verschiedene Exponenten r, t

$$S^r = U S^t U^{-1},$$

so ergiebt sich, wenn $U = \begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$ gesetzt wird, als Bedingung

$$\sigma^r \lambda = \pm \sigma^t \lambda, \quad \sigma^r \mu = \pm \sigma^{-t} \mu$$
$$\sigma^{-r} \nu = \pm \sigma^t \nu, \quad \sigma^{-r} \varrho = \pm \sigma^{-t} \varrho,$$

wo überall dasselbe Zeichen gelten muss. Daraus folgt, dass entweder

$$\sigma^r = \pm \sigma^t, \quad \nu = 0, \quad \mu = 0, \quad \lambda \varrho = 1$$

oder

$$\sigma^r = \pm \sigma^{-t}, \quad \lambda = 0, \quad \varrho = 0, \quad \mu \nu = -1$$

sein muss, und dann ergiebt sich:

$$U S U^{-1} = S \quad \text{oder} \quad = S^{-1},$$

und in beiden Fällen stimmen also die beiden Cyklen (12) vollständig mit einander überein.

Hiernach ergiebt sich aus den Zahlen am Schluss des §. 68 für die Anzahl der Cyklen erster, zweiter und dritter Art:

$$p + 1, \quad \frac{p(p+1)}{2}, \quad \frac{p(p-1)}{2}.$$

Es ist zweckmässig, neben den Gruppen L_p und A_p noch eine dritte Gruppe in $E_{2,p}$ zu betrachten, die mit diesen isomorph ist, wenn sie sich auch nicht durch Transformation darauf zurückführen lässt.

Da N reell ist, so können wir nach §. 67 eine Zahl ν in $\mathfrak{E}_{2,p}$ so bestimmen, dass $N = \nu^{p+1}$ ist. Wir lassen nun der Substitution

$$A = \begin{pmatrix} \alpha, & \beta \\ -N\beta^p, & \alpha^p \end{pmatrix}$$

aus A_p eine Substitution B entsprechen, die so gebildet ist:

$$(13) \qquad B = \begin{pmatrix} \alpha, & \nu\beta \\ -\nu^p \beta^p, & \alpha^p \end{pmatrix}, \quad \alpha^{p+1} + N\beta^{p+1} = 1.$$

Setzen wir zwei Substitutionen B, B_1 von der Form (13) zusammen, so erhalten wir

$$B B_1 = \begin{pmatrix} \alpha, & \nu\beta \\ -\nu^p \beta^p, & \alpha^p \end{pmatrix} \begin{pmatrix} \alpha_1, & \nu\beta_1 \\ -\nu^p \beta_1^p, & \alpha_1^p \end{pmatrix}$$
$$= \begin{pmatrix} \alpha\alpha_1 - N\beta\beta_1^p, & \nu(\alpha\beta_1 + \beta\alpha_1^p) \\ -\nu^p(\beta^p\alpha_1 + \alpha^p\beta_1^p), & \alpha^p\alpha_1^p - N\beta^p\beta_1 \end{pmatrix};$$

darin sind

$$\alpha\alpha_1 - N\beta\beta_1^p, \quad \alpha^p\alpha_1^p - N\beta^p\beta_1 \quad \text{und} \quad \alpha\beta_1 + \beta\alpha_1^p, \quad \beta^p\alpha_1 + \alpha^p\beta_1^p$$

zwei conjugirte Paare, und daher hat $B B_1$ auch die Form (13) und steht in derselben Beziehung zu $A A_1$, wie B zu A und B_1 zu A_1.

Daraus geht hervor, dass die Gesammtheit der Substitutionen B eine mit $\varDelta_p$ isomorphe Gruppe bildet, und diese Gruppe wollen wir mit Γ_p bezeichnen.

Setzen wir β an Stelle von $\nu\beta$ und bezeichnen mit α', β' die zu α, β conjugirten Grössen, so können wir die Substitutionen der Gruppe Γ_p auch in der einfacheren Form annehmen:

$$(14) \qquad B = \begin{pmatrix} \alpha, & \beta \\ -\beta', & \alpha' \end{pmatrix}, \quad \alpha\alpha' + \beta\beta' = 1.$$

Um von einer dieser Substitutionen B zu der entsprechenden reellen Substitution A überzugehen, leitet man zunächst aus (14) die entsprechende Substitution $\varDelta$ her:

$$(15) \qquad \varDelta = \begin{pmatrix} \alpha, & \nu^{-1}\beta \\ -\nu\beta', & \alpha' \end{pmatrix},$$

und bildet daraus nach (3) und (7):

$$(16) \qquad A = R \varDelta R^{-1}.$$

Trotz des Isomorphismus lässt sich die Gruppe Γ_p nicht in L_p oder $\varDelta_p$ transformiren, wenigstens nicht durch Substitutionen, deren Zahlen dem Körper $\mathfrak{G}_{2,p}$ angehören. Man müsste, um die Transformation auszuführen, in einen höheren Körper gehen, in dem alle Zahlen von $\mathfrak{G}_{2,p}$ Quadrate sind.

§. 70.

Divisoren der Gruppe L_p, deren Grad durch p theilbar ist.

Es ist ein Problem von grösstem Interesse, alle Divisoren der Gruppe L_p zu bestimmen. Von der Lösung dieses Problems hängt es ab, in welcher Weise man die Gruppe L_p durch Permutationen von Ziffern darstellen kann, bei welchen algebraischen Gleichungen also diese Gruppen auftreten können (§. 28, 2.).

Die cyklischen Gruppen, die in L_p enthalten sind, haben wir in den vorangehenden Paragraphen schon betrachtet. Wir haben gesehen, dass der Grad einer cyklischen Gruppe entweder gleich p oder ein Theiler von $^1/_2\,(p-1)$ oder von $^1/_2\,(p+1)$

ist, und jeder Theiler dieser Zahlen tritt auch unter den Graden der cyklischen Gruppen auf. Der Index eines cyklischen Theilers kann niemals kleiner sein als $\frac{1}{2}(p^2-1)$, $p(p+1)$, $p(p-1)$.

Wenn der Grad eines Theilers G von L_p durch p theilbar ist, so enthält er eine cyklische Gruppe vom Grade p, und wir können nach §. 68 die Gruppe G so transformiren, dass diese cyklische Gruppe aus den Substitutionen

$$T = \begin{pmatrix} 1, & t \\ 0, & 1 \end{pmatrix}, \quad t = 0, 1, 2, \ldots, p-1$$

besteht. Wenn nun G noch eine Substitution

$$A = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$$

enthält, in der c von Null verschieden ist, so kommt darin auch

$$(1) \qquad \begin{pmatrix} 1, & -a c^{-1} \\ 0, & 1 \end{pmatrix} \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \begin{pmatrix} 1, & -d c^{-1} \\ 0, & 1 \end{pmatrix} = \begin{pmatrix} 0, & -c^{-1} \\ c, & 0 \end{pmatrix}$$

vor. Daraus folgt weiter, dass auch

$$\begin{pmatrix} 0, & -c^{-1} \\ c, & 0 \end{pmatrix} \begin{pmatrix} 1, & t \\ 0, & 1 \end{pmatrix} \begin{pmatrix} 0, & -c^{-1} \\ c, & 0 \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ -c^2 t, & 1 \end{pmatrix},$$

und mithin jede Substitution

$$U = \begin{pmatrix} 1, & 0 \\ u, & 1 \end{pmatrix}, \quad u = 0, 1, 2, \ldots, p-1$$

vorkommt. Setzt man U für $u = -1$ an Stelle von A in die Formel (1), so folgt, dass G auch die Substitution $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$ enthält, die mit U zusammen ein System erzeugender Elemente von L_p giebt (§. 65), so dass also G mit L_p identisch ist. Es folgt hieraus, dass G, wenn es nicht mit L_p identisch sein soll, nur Substitutionen von der Form

$$A = \begin{pmatrix} a, & b \\ 0, & a^{-1} \end{pmatrix}$$

enthalten kann. Umgekehrt bilden alle diese Substitutionen eine Gruppe vom Grade $\frac{1}{2}p(p-1)$, also einen Theiler vom Index $p+1$.

Es sind darunter noch gewisse Theiler von grösserem Index enthalten, die man erhält, wenn man für a nicht alle Werthe nimmt, sondern alle Werthe von der Form a^s, wenn s ein Theiler von $\frac{1}{2}(p-1)$ ist. Der Grad einer solchen Gruppe ist $\frac{1}{2}p(p-1):s$.

Fassen wir die Gruppe L_p als Gruppe der linearen Substitutionen

$$\eta = \frac{a\,\xi + b}{c\,\xi + d}$$

auf, und lassen darin ξ, η nach §. 65 die Zahlen $\infty, 0, 1, \ldots, p-1$ durchlaufen, so giebt uns G die Gruppe der ganzen linearen Substitutionen

$$\eta = a^2\,\xi + a\,b.$$

Das sind die Substitutionen, die die Ziffer ∞ ungeändert lassen, und also eine Permutationsgruppe von nur p Ziffern liefern. Es sind dies dieselben speciellen metacyklischen Gruppen, die wir im siebzehnten Abschnitte des ersten Bandes betrachtet haben.

Die verschiedenen aus G transformirten Gruppen lassen irgend einen der übrigen $p+1$ Indices ungeändert, und die Gesammtzahl dieser Gruppen ist $p+1$.

§. 71.

Divisoren der Gruppe L_p, deren Grad nicht durch p theilbar ist.

Um die übrigen Theiler von L_p zu finden, deren Grad nicht durch p theilbar ist, können wir Schritt für Schritt denselben Weg gehen, der uns im siebenten und achten Abschnitte zu der Bestimmung der Polyëdergruppen geführt hat. Wir können uns hier damit begnügen, die Hauptmomente der Ableitung hervorzuheben und wegen der Beweise auf die genannte Stelle zu verweisen, wo ganz dieselben Schlüsse zu machen waren.

Es ist hierzu erforderlich, die Gruppe L_p, wie im §. 65 aus einander gesetzt, als Gruppe linearer gebrochener Substitutionen

$$(1) \qquad \Theta(\xi) = \frac{a\,\xi + b}{c\,\xi + d}$$

aufzufassen, und darin der Veränderlichen ξ alle p^2+1 Zahlenwerthe des Congruenzkörpers $\mathfrak{E}_{2,p}$, einschliesslich ∞, beizulegen. Dadurch gewinnen wir den Vortheil, dass die Gleichung

$$(2) \qquad \xi = \frac{a\,\xi + b}{c\,\xi + d}$$

immer zwei Wurzeln hat. Diese beiden Wurzeln sind von einander verschieden, wenn wir Substitutionen p^{ten} Grades ausschliessen, die ja in einer Gruppe, deren Grad nicht durch p theilbar ist, nicht vorkommen können, und die nach §. 68, 1. die einzigen sind, für welche die beiden Wurzeln von (2) zusammenfallen.

Diese beiden Wurzeln nennen wir die Pole von Θ.

Wir untersuchen eine Gruppe G, deren Grad n nicht durch p theilbar ist, die ein Theiler von L_p sein soll. Wenn in G die Substitutionen

$$\Theta_1, \Theta_2, \ldots, \Theta_{\nu-1},$$

aber keine anderen vorkommen, die denselben Pol α haben, so nennen wir α einen ν-zähligen Pol (§. 52).

Ist nun S irgend eine Substitution der Gruppe $\mathfrak{G}_{2,p}$, so erhalten wir, wenn wir L_p durch S^{-1} transformiren, eine mit L_p isomorphe Gruppe $S L_p S^{-1}$, und G geht durch dieselbe Transformation in eine isomorphe Gruppe $S G S^{-1}$ über.

Obwohl die Substitutionen dieser letzteren Gruppe keine reellen Coëfficienten haben, so hat doch jede von ihnen zwei Pole, die man erhält, wenn man die Substitution S auf die Pole von Θ anwendet. Denn es ist, wenn α ein Pol von Θ ist:

$$S \Theta S^{-1} S(\alpha) = S \Theta(\alpha) = S(\alpha).$$

Wir haben also, wie in §. 51, 2.:

1. **Die Gruppe G lässt sich so transformiren, dass eine beliebige ihrer Substitutionen die Pole 0 und ∞ erhält, dass also diese Substitution multiplicativ wird.**

Wir führen nun der Reihe nach die Sätze des §. 52 auf, soweit sie hier in Frage kommen, und werden nur da, wo die veränderten Voraussetzungen es erfordern, eine Ausführung hinzufügen:

2. **Ist α ein ν-zähliger Pol, so bilden die Substitutionen 1, $\Theta_1, \Theta_2, \ldots, \Theta_{\nu-1}$ eine cyklische Gruppe. Ihre Substitutionen können alle (durch Transformation) in die Form gesetzt werden:**

$$(3) \qquad \Theta(\xi) = \gamma^{h \frac{p^2-1}{\nu}} \xi, \quad h = 0, 1, \ldots, \nu - 1 \text{ (§. 52, 3.)}.$$

Hierin bedeutet γ eine primitive Wurzel, also $\gamma^{\frac{p^2-1}{\nu}}$ eine primitive ν^{te} Einheitswurzel des Congruenzkörpers $\mathfrak{G}_{2,p}$ (§. 67).

3. Beide Pole einer Substitution Θ sind gleichzählig (§. 52, 4.).

Ist Q die cyklische Gruppe ν^{ten} Grades der Potenzen von Θ und $n = \nu\mu$, so erhält man

$$G = Q + \psi_1 Q + \cdots + \psi_{\mu-1} Q,$$

worin $\psi_1, \ldots, \psi_{\mu-1}$ Substitutionen aus G sind, und

4. die Zahlen

$$(4) \qquad \alpha,\ \psi_1(\alpha) = \alpha_1,\ \psi_2(\alpha) = \alpha_2, \ldots, \psi_{\mu-1}(\alpha) = \alpha_{\mu-1}$$

bilden ein System gleichzähliger conjugirter Pole der Gruppe G.

Die sämmtlichen Pole der Gruppe G lassen sich also in Systeme conjugirter Pole zusammenfassen, und wir bekommen so die unbestimmte Gleichung

$$(5) \qquad \begin{aligned} 2n - 2 &= \mu(\nu - 1) + \mu'(\nu' - 1) + \mu''(\nu'' - 1) \ldots \\ &= nh - \mu - \mu' - \mu'' \ldots, \end{aligned}$$

wenn h die Anzahl der Systeme conjugirter Pole ist, und von dieser Gleichung haben wir in §. 52 gesehen, dass sie nur eine beschränkte Anzahl von Lösungen zulässt.

Um die diesen Lösungen entsprechenden Theiler der Congruenzgruppen zu finden, können wir geradezu in den Formeln der Polyëdergruppen, die im achten Abschnitte aufgestellt sind, für die darin vorkommenden Einheitswurzeln die in §. 67 definirten Einheitswurzeln des Körpers $\mathfrak{G}_{2,p}$ setzen, mit denen ja nach denselben Regeln gerechnet wird. Dabei können natürlich nur solche Einheitswurzeln vorkommen, deren Grad ein Theiler von $p^2 - 1$ ist. Es ist schliesslich bei jeder solchen Gruppe noch zu untersuchen, ob ihre Substitutionen in L_p oder in einer damit isomorphen Gruppe enthalten sind. Wir haben dann folgende Fälle von Lösungen der Gleichung (5), wobei γ stets eine primitive Wurzel des Körpers $\mathfrak{G}_{2,p}$ bedeutet (§. 55).

I. Cyklische Gruppen vom Grade n, $\quad h = 2,\ \nu = \nu' = n,\ \mu = \mu' = 1$

$$C_n = \begin{pmatrix} \gamma^{\frac{p^2-1}{2n}\lambda}, & 0 \\ 0, & \gamma^{-\frac{(p^2-1)}{2n}\lambda} \end{pmatrix}, \qquad \lambda = 0, 1, \ldots, n-1.$$

Diese Gruppe ist reell, wenn n ein Theiler von $\frac{1}{2}(p-1)$ ist, weil dann und nur dann die Exponenten von γ durch $p-1$ theilbar sind. Die Gruppe ist in Γ_p und zugleich in Δ_p (§. 69) enthalten, wenn $\gamma^{\frac{p^2-1}{2n}}$, $\gamma^{-\frac{p^2-1}{2n}}$ conjugirt sind, wenn also

$$\gamma^{-\frac{p^2-1}{2n}} = \gamma^{p\frac{p^2-1}{2n}} \quad \text{oder} \quad \gamma^{(p+1)\frac{p^2-1}{2n}} = 1$$

ist, d. h. wenn n ein Theiler von $\frac{1}{2}(p+1)$ ist. Dies stimmt mit §. 68 überein, wonach andere cyklische Gruppen, als solche, deren Grad gleich p oder ein Theiler von $\frac{1}{2}(p-1)$ oder $\frac{1}{2}(p+1)$ ist, nicht vorkommen. In den übrigen Polyëdergruppen ist $h=3$, und wir haben:

II. Diëdergruppen vom Grade $2m$, $\begin{array}{l}\nu=\nu'=2,\ \nu''=m\\ \mu=\mu'=m,\ \mu''=2\end{array}$

$$D_m = \begin{pmatrix} \gamma^{\frac{p^2-1}{2m}\lambda}, & 0 \\ 0, & \gamma^{-\frac{p^2-1}{2m}\lambda} \end{pmatrix}, \begin{pmatrix} 0, & \gamma^{\frac{p^2-1}{2m}\lambda} \\ -\gamma^{-\frac{p^2-1}{2m}\lambda}, & 0 \end{pmatrix}, \ \lambda = 0, 1, \ldots, m-1.$$

Diese Gruppe ist in L_p enthalten, wenn $p \equiv 1 \pmod{2m}$, und in Γ_p, wenn $p \equiv -1 \pmod{2m}$, wie im Falle I.

Hier ist die in §. 55 gegebene zweite Darstellung der Diëdergruppe gewählt, in der die Unterscheidung der Fälle etwas einfacher wird, als bei der ersten.

III. Tetraëdergruppe, $\begin{array}{l}\nu=2,\ \nu'=3,\ \nu''=3,\ n=12\\ \mu=6,\ \mu'=4,\ \mu''=4.\end{array}$

Um diese Gruppe darzustellen, bemerken wir, dass im Körper $\mathfrak{E}_{2,p}$ immer eine 8te Einheitswurzel $\gamma^{\frac{p^2-1}{8}}$ existirt. Wir erhalten also nach §. 56 die drei erzeugenden Substitutionen

$$\Theta = \begin{pmatrix} \gamma^{\frac{p^2-1}{4}}, & 0 \\ 0, & \gamma^{-\frac{p^2-1}{4}} \end{pmatrix}, \ \psi = \begin{pmatrix} 0, & \gamma^{\frac{p^2-1}{4}} \\ -\gamma^{-\frac{p^2-1}{4}}, & 0 \end{pmatrix}, \ \psi_1 = \psi\,\Theta = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$

$$\chi = \begin{pmatrix} \frac{1}{\sqrt{-2}}\gamma^{\frac{p^2-1}{8}}, & \frac{1}{\sqrt{-2}}\gamma^{\frac{p^2-1}{8}} \\ \frac{1}{\sqrt{-2}}\gamma^{-\frac{p^2-1}{8}}, & -\frac{1}{\sqrt{-2}}\gamma^{-\frac{p^2-1}{8}} \end{pmatrix}.$$

1) Ist $p \equiv 1 \pmod 4$, so ist $\gamma^{\frac{p^2-1}{4}}$ reell, und $\gamma^{\frac{p^2-1}{8}}$ ist reell oder rein imaginär, je nachdem $p \equiv 1$ oder $\equiv 5 \pmod 8$ ist.

Uebereinstimmend damit ist auch $\sqrt{-2}$ reell oder rein imaginär (Bd. I, §. 138, 4., 6.), und folglich ist in diesen Fällen Θ, ψ, χ und mithin die ganze Tetraëdergruppe reell.

2) Ist aber $p \equiv 3 \pmod 4$, so sind $\gamma^{\frac{p^2-1}{4}}$, $\gamma^{-\frac{p^2-1}{4}}$ conjugirt imaginär, weil $\gamma^{(p+1)\frac{p^2-1}{4}} = 1$ ist.

Ist $p \equiv 3 \pmod 8$, so ist $\sqrt{-2}$ reell und $\gamma^{\frac{p^2-1}{8}(p+1)} = -1$, also $\gamma^{\frac{p^2-1}{8}}$ und $-\gamma^{\frac{p^2-1}{8}}$ conjugirt imaginär, und ist $p \equiv 7 \pmod 8$, so ist $\sqrt{-2}$ rein imaginär, $\gamma^{\frac{p^2-1}{8}}$ und $\gamma^{-\frac{p^2-1}{8}}$ conjugirt imaginär, und folglich gehört Θ, ψ_1, χ in diesen Fällen zur Gruppe Γ_p. Es giebt also in allen Fällen in der Gruppe L_p eine Tetraëdergruppe.

Für $p = 5$ z. B. kann man, da -2 quadratischer Nichtrest von 5 ist, $\varepsilon = \sqrt{-2}$, und, da ± 2 die beiden primitiven Wurzeln von 5 sind, etwa

$$\gamma^6 = -2, \quad \gamma^3 = \sqrt{-2}, \quad \gamma = 1 + \sqrt{-2}$$

setzen, dann folgt

$$(6) \qquad \Theta = \begin{pmatrix} 2, & 0 \\ 0, & 3 \end{pmatrix}, \quad \psi = \begin{pmatrix} 0, & 2 \\ 2, & 0 \end{pmatrix}, \quad \psi_1 = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$
$$\chi = \begin{pmatrix} 1, & 1 \\ 2, & -2 \end{pmatrix}, \quad \chi^2 = \begin{pmatrix} 2, & 1 \\ 2, & -1 \end{pmatrix},$$

und daraus ergiebt sich die gesuchte Tetraëdergruppe für $p = 5$ [§. 56, (3)]:

$$(7) \qquad \begin{matrix} \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, & \begin{pmatrix} 2, & 0 \\ 0, & -2 \end{pmatrix}, & \begin{pmatrix} 0, & 2 \\ 2, & 0 \end{pmatrix}, & \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \\ \begin{pmatrix} 1, & 1 \\ 2, & -2 \end{pmatrix}, & \begin{pmatrix} 2, & 2 \\ 1, & -1 \end{pmatrix}, & \begin{pmatrix} -1, & 1 \\ 2, & 2 \end{pmatrix}, & \begin{pmatrix} -2, & 2 \\ 1, & 1 \end{pmatrix} \\ \begin{pmatrix} 2, & 1 \\ 2, & -1 \end{pmatrix}, & \begin{pmatrix} -1, & 2 \\ 1, & 2 \end{pmatrix}, & \begin{pmatrix} 1, & 2 \\ 1, & -2 \end{pmatrix}, & \begin{pmatrix} -2, & 1 \\ 2, & 1 \end{pmatrix}. \end{matrix}$$

Diese Gruppe ist ein Theiler von L_5 vom Index 5.

IV. Octaëdergruppe.

In der Octaëdergruppe ist eine cyklische Gruppe vom Grade 4 enthalten, und eine solche Gruppe kann also nur existiren, wenn $\frac{1}{2}(p-1)$ oder $\frac{1}{2}(p+1)$ durch 4 theilbar, d. h. wenn $p \equiv \pm 1 \pmod 8$ ist.

Unter dieser Voraussetzung führen die Formeln §. 57 zur Aufstellung einer Octaëdergruppe.

Die erzeugenden Substitutionen sind:

$$\Theta = \begin{pmatrix} \gamma^{\frac{p^2-1}{8}}, & 0 \\ 0, & \gamma^{-\frac{p^2-1}{8}} \end{pmatrix}, \quad \psi = \begin{pmatrix} 0, & \gamma^{\frac{p^2-1}{4}} \\ \gamma^{\frac{p^2-1}{4}}, & 0 \end{pmatrix}$$

(8)

$$\chi = \begin{pmatrix} \frac{1}{\sqrt{2}}\gamma^{-\frac{p^2-1}{8}}, & \frac{1}{\sqrt{2}}\gamma^{-\frac{p^2-1}{8}} \\ \frac{-1}{\sqrt{2}}\gamma^{\frac{p^2-1}{8}}, & \frac{1}{\sqrt{2}}\gamma^{\frac{p^2-1}{8}} \end{pmatrix}.$$

Diese Gruppe ist reell, wenn $p \equiv 1 \pmod 8$ ist, und imaginär, aber in Γ_p enthalten, wenn $p \equiv -1 \pmod 8$ ist.

Das erste Beispiel ist $p = 7$. Hier ist -1 quadratischer Nichtrest, und man kann also $\varepsilon = \sqrt{-1} = i$ setzen. Nehmen wir $\gamma = 2 + i$, $\gamma^7 = 2 - i$, $\gamma^6 = 2(1 + i)$, $\gamma^8 = 5$, so ist γ eine primitive Wurzel, da $\gamma, \gamma^2, \ldots, \gamma^7$ von einander verschieden sind und 5 reelle primitive Wurzel von 7 ist, so dass jede nicht verschwindende Zahl des Körpers $\mathfrak{C}_{2,7}$ in der Form

$$5^\mu \gamma^\nu = \gamma^{8\mu+\nu}$$

dargestellt werden kann, wenn

$$\mu = 0, 1, 2, 3, 4, 5,$$
$$\nu = 0, 1, 2, 3, 4, 5, 6, 7$$

gesetzt wird.

Es ist dann ferner $\sqrt{2} = 3$, und folglich sind die Substitutionen Θ, ψ, χ:

$$(9) \quad \begin{pmatrix} 2(1+i), & 0 \\ 0, & 2(1-i) \end{pmatrix}, \begin{pmatrix} 0, & i \\ i, & 0 \end{pmatrix}, \begin{pmatrix} 4(1-i), & 4(1-i) \\ -4(1+i), & 4(1+i) \end{pmatrix}.$$

Will man zur reellen Form übergehen, so muss man nach §. 69 verfahren. Man geht von den Substitutionen B zu den A über, indem man $\nu = \gamma^3 = 2 - 3i$ setzt, und erhält aus (9) für Θ, ψ, χ in der Gruppe A_p:

$$(10) \quad \begin{pmatrix} 2+2i, & 0 \\ 0, & 2-2i \end{pmatrix}, \begin{pmatrix} 0, & 3-2i \\ 3+2i, & 0 \end{pmatrix}, \begin{pmatrix} 4-4i, & 1-4i \\ 1+4i, & 4+4i \end{pmatrix}.$$

Hier ist ferner

$$R = \begin{pmatrix} 4, & 4i \\ i, & 1 \end{pmatrix}$$

zu setzen, woraus sich durch Bildung von RAR^{-1} die erzeugenden Substitutionen der Octaëdergruppe in reeller Form ergeben:

$$(11)\quad \begin{gathered} \Theta = \begin{pmatrix} 2, 1 \\ 3, 2 \end{pmatrix}, \quad \psi = \begin{pmatrix} 2, & 2 \\ 1, & -2 \end{pmatrix}, \quad \omega = \psi\Theta = \begin{pmatrix} 3, & -1 \\ 3, & -3 \end{pmatrix} \\ \chi = \begin{pmatrix} 0, 2 \\ 3, 1 \end{pmatrix}, \quad \chi^2 = \begin{pmatrix} -1, 2 \\ 3, 0 \end{pmatrix}. \end{gathered}$$

Nun ist es leicht, nach §. 57 die vollständige Gruppe zu bilden, was nicht nöthig ist, weiter auszuführen.

Die Octaëdergruppe für $p = 7$ ist ein Theiler von L_7 vom Index 7.

V. Ikosaëdergruppe.

In dem Falle $p = 5$ ist L_p selbst eine Ikosaëdergruppe. Für andere Werthe von p kann nur dann eine Ikosaëdergruppe in L_p enthalten sein, wenn $p^2 - 1$ durch 5 theilbar, also $p \equiv \pm 1 \pmod 5$ ist. Dann erhalten wir aus §. 58 die erzeugenden Substitutionen einer solchen Gruppe.

Setzen wir zur Abkürzung

$$\gamma^{\frac{p^2-1}{10}} = \varrho,$$

so haben wir ϱ^2 für ε in die Formeln des §. 58 einzusetzen, und erhalten

$$(12)\quad \begin{gathered} \Theta = \begin{pmatrix} \varrho, 0 \\ 0, \varrho^{-1} \end{pmatrix}, \quad \psi = \begin{pmatrix} 0, 1 \\ -1, 0 \end{pmatrix} \\ \chi = \begin{pmatrix} \dfrac{-1}{\varrho^2 - \varrho^{-2}}, & \dfrac{1}{\varrho - \varrho^{-1}} \\ \dfrac{1}{\varrho - \varrho^{-1}}, & \dfrac{1}{\varrho^2 - \varrho^{-2}} \end{pmatrix} \quad [\S.\ 58,\ (26)]. \end{gathered}$$

Ist $p \equiv 1 \pmod 5$, so ist ϱ, und damit die ganze Gruppe reell. Ist aber $p \equiv -1 \pmod 5$, so sind ϱ und ϱ^{-1} conjugirt, und folglich ist die gefundene Gruppe in Γ_p enthalten, und um die Ikosaëdergruppe in L_p zu erhalten, müssen wir erst nach §. 69 transformiren.

Für $p = 11$ erhalten wir unmittelbar eine reelle Ikosaëdergruppe vom Index 11.

Wir können für $\varrho = \gamma^{12}$ eine beliebige primitive Wurzel von 11, z. B. 8, wählen. Dann wird $\varrho^{-1} = 7$ und

$$\varrho - \varrho^{-1} = 1, \quad \varrho^2 - \varrho^{-2} = 4,$$

also

$$\text{(13)} \qquad \Theta = \begin{pmatrix} 3, & 0 \\ 0, & 4 \end{pmatrix}, \quad \psi = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad \chi = \begin{pmatrix} -3, & 1 \\ 1, & 3 \end{pmatrix}.$$

Damit ist also festgestellt, welche Arten von Theilern in der Gruppe L_p vorkommen können, und es ist auch gezeigt, dass alle diese Theiler wirklich vorhanden sind. Die Frage, wie man für jeden Typus alle überhaupt möglichen Theiler erhält, haben wir hier bei Seite gelassen. Wir wollen darüber nur noch folgende Bemerkungen machen.

Wenn man eine gefundene Gruppe G durch irgend eine Substitution der Gruppe L_p transformirt, so erhält man einen conjugirten Theiler. Wenn man aber durch eine imaginäre Substitution der Gruppe E_p transformirt, so kann es vorkommen, dass die transformirte Gruppe von G trotzdem reell wird und nicht mit G innerhalb L_p conjugirt (wiewohl beide conjugirte Theiler von E_p sind). So erhält man allgemein aus der Octaëder- und der Ikosaëdergruppe eine zweite nicht conjugirte, wenn man mit $\begin{pmatrix} \varepsilon, & 0 \\ 0, & \varepsilon^{-1} \end{pmatrix}$ transformirt. Bei der Tetraëdergruppe giebt dies nur dann eine neue Gruppe, wenn $p \equiv \pm 1 \pmod 8$ ist. Die zweite Gruppe ergiebt sich nach der Formel:

$$\text{(14)} \qquad \begin{pmatrix} \varepsilon, & 0 \\ 0, & \varepsilon^{-1} \end{pmatrix} \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \begin{pmatrix} \varepsilon^{-1}, & 0 \\ 0, & \varepsilon \end{pmatrix} = \begin{pmatrix} a, & bN \\ cN^{-1}, & d \end{pmatrix} \quad (N = \varepsilon^2).$$

Um diese Verhältnisse an den Beispielen $p = 5, 7, 11$ aufzuweisen, ist es zweckmässig, die oben gefundene Gruppe (6) für $p = 7$ so zu transformiren, dass die Substitution χ, die von der dritten Ordnung ist, die Normalform S erhält. Man findet diese Transformation leicht, und erhält für diesen Fall:

$$\text{(15)} \qquad \begin{aligned} \begin{pmatrix} 1, & 1 \\ -2, & -1 \end{pmatrix} \begin{pmatrix} 0, & 2 \\ 3, & 1 \end{pmatrix} \begin{pmatrix} -1, & -1 \\ 2, & 1 \end{pmatrix} &= \begin{pmatrix} 3, & 0 \\ 0, & 5 \end{pmatrix} = \chi' \\ \begin{pmatrix} 1, & 1 \\ -2, & -1 \end{pmatrix} \begin{pmatrix} 2, & 1 \\ 3, & 2 \end{pmatrix} \begin{pmatrix} -1, & -1 \\ 2, & 1 \end{pmatrix} &= \begin{pmatrix} 1, & -2 \\ -1, & 3 \end{pmatrix} = \Theta' \\ \begin{pmatrix} 1, & 1 \\ -2, & -1 \end{pmatrix} \begin{pmatrix} 2, & 2 \\ 1, & -2 \end{pmatrix} \begin{pmatrix} -1, & -1 \\ 2, & 1 \end{pmatrix} &= \begin{pmatrix} -3, & -3 \\ 1, & 3 \end{pmatrix} = \psi', \end{aligned}$$

woraus man durch Zusammensetzung

$$\psi'\Theta'\chi' = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \tag{16}$$

erhält. Wir können demnach in den drei Fällen folgende erzeugende Substitutionen der Tetraëder-, Octaëder- und Ikosaëdergruppe [(6), (13), (15)] annehmen:

$$p = 5. \quad \begin{pmatrix} 2, & 0 \\ 0, & 3 \end{pmatrix}, \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \begin{pmatrix} 2, & 2 \\ 1, & -1 \end{pmatrix}$$

$$p = 7. \quad \begin{pmatrix} 3, & 0 \\ 0, & 5 \end{pmatrix}, \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \begin{pmatrix} 1, & -2 \\ -1, & 3 \end{pmatrix}$$

$$p = 11. \quad \begin{pmatrix} 3, & 0 \\ 0, & 4 \end{pmatrix}, \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \begin{pmatrix} -3, & 1 \\ 1, & 3 \end{pmatrix}.$$

Durch wiederholte Zusammensetzung, die sich auf sehr verschiedene Arten anordnen lässt, ergeben sich hieraus leicht die vollständigen Gruppen:

$$p = 5.$$

$$\begin{pmatrix} x, & 0 \\ 0, & x^{-1} \end{pmatrix}, \begin{pmatrix} 0, & x \\ -x^{-1}, & 0 \end{pmatrix}, \begin{pmatrix} x, & y \\ 2y^{-1}, & 3x^{-1} \end{pmatrix} \quad \begin{matrix} x = 1, 2 \\ y = \pm 1, \pm 2 \end{matrix}$$

$$p = 7.$$

$$\begin{pmatrix} x, 0 \\ 0, x^{-1} \end{pmatrix}, \begin{pmatrix} 0, & x \\ -x^{-1}, 0 \end{pmatrix}, \begin{pmatrix} x, & -xz \\ -2x^{-1}z^{-1}, & 3x^{-1} \end{pmatrix}, \begin{pmatrix} xz, & x \\ -3x^{-1}, & -2x^{-1}z^{-1} \end{pmatrix}$$

$$x = 1, 2, 3; \quad z = 1, 2, 4$$

(z quadratischer Rest von 7).

$$p = 11.$$

$$\begin{pmatrix} x, 0 \\ 0, x^{-1} \end{pmatrix}, \begin{pmatrix} 0, & x \\ -x^{-1}, 0 \end{pmatrix}, \begin{pmatrix} x, & -xz \\ -x^{-1}z^{-1}, & 2x^{-1} \end{pmatrix}, \begin{pmatrix} xz, & x \\ -2x^{-1}, & -x^{-1}z^{-1} \end{pmatrix}$$

$$x = 1, 2, 3, 4, 5; \quad z = 1, 3, 4, 5, 9$$

(z quadratischer Rest von 11).

Die Anwendung der Transformation (14) führt bei $p = 5$ zu keiner neuen Gruppe; bei $p = 7, 11$ erhält man je eine andere Gruppe, die aus diesen hervorgeht, wenn man für z die Reihe der quadratischen Nichtreste statt der Reste setzt [1]).

---

[1]) Die Eigenschaft der Congruenzgruppen, einfach zu sein, hat schon Galois gekannt. Ebenso waren ihm die Theiler vom Index p für $p = 5, 7, 11$ bekannt. Eingehender untersucht sind diese Gruppen von

§. 72.

Constitution der Gruppe L_7 vom Grade 168.

Unter den hier gefundenen einfachen Gruppen ist die nächste nach der Ikosaëdergruppe, die hier als L_5 wiederkehrt, die Gruppe L_7 vom Grade 168, die, wie wir gesehen haben, eine Octaëdergruppe als Theiler enthält. Da uns diese merkwürdige Gruppe später noch mehrfach begegnen wird, so wollen wir hier noch etwas näher auf ihren Bau eingehen.

Im §. 57 ist die Octaëdergruppe durch drei Elemente χ, ω, Θ in der Form dargestellt:

$$(1) \qquad \chi^\lambda \omega^\mu \Theta^\nu, \quad \lambda = 0, 1, 2; \; \mu = 0, 1; \; \nu = 0, 1, 2, 3.$$

Zwischen diesen Elementen bestehen die Relationen

$$(2) \quad \omega\chi = \chi^2\omega, \quad \Theta\omega = \omega\Theta^3, \quad \Theta\chi = \chi^2\omega\Theta^2, \quad \Theta^2\chi = \chi\omega\Theta^3,$$

und diese Bedingungen haben wir, wenn noch die Grade 3, 2, 4 der Elemente χ, ω, Θ hinzukommen, als ausreichend nachgewiesen, um das System (1) als Octaëdergruppe zu charakterisiren.

Aus (2) haben wir im §. 57 als Folgerungen die Formeln abgeleitet:

$$(3) \quad \begin{array}{llll} \omega\chi = \chi^2\omega, & \omega\chi^2 = \chi\omega, & \Theta^2\chi^2 = \chi^2\omega\Theta, & \\ \Theta\chi = \chi^2\omega\Theta^2, & \Theta^2\chi = \chi\omega\Theta^3, & \Theta^3\chi = \chi^2\Theta, & \\ \Theta\omega = \omega\Theta^3, & \Theta^2\omega = \omega\Theta^2, & \Theta^3\omega = \omega\Theta, & \Theta\chi^2 = \chi\Theta^3, \end{array}$$

die wir später mehrfach benutzen werden.

Im §. 71 haben wir die Octaëdergruppe auch als Congruenzgruppe nach dem Modul 7 dargestellt und haben in den dortigen Formeln (11)

$$(4) \qquad \chi = \begin{pmatrix} 0, & 2 \\ 3, & 1 \end{pmatrix}, \quad \omega = \begin{pmatrix} 3, & -1 \\ 3, & -3 \end{pmatrix}, \quad \Theta = \begin{pmatrix} 2, & 1 \\ 3, & 2 \end{pmatrix}$$

gefunden. Für das Folgende ist es aber, im Interesse einer einfacheren Rechnung, zweckmässig, diese Gruppe noch zu trans-

Serret (Cours d'algèbre supérieure) und von C. Jordan (Traité des Substitutions). Vergl. Weber, Elliptische Functionen etc., §. 84 f. Die vollständige Aufstellung aller Theiler rührt von Gierster her (Math. Ann., Bd. XVIII). Ausführliche Behandlung der Congruenzgruppen in „Klein-Fricke, Vorlesungen über die Theorie der elliptischen Modulfunctionen". Bd. I, Leipzig 1890.

formiren. Es hat sich nämlich früher schon gezeigt, dass in der Gruppe L_7 Theiler vom Grade 21 enthalten sind, deren Index $= 8$ ist, und die gerade für unseren Zweck von besonderer Wichtigkeit sind. Unter den conjugirten Theilern des Index 8 ist aber der einfachste und für die Rechnung bequemste der aus allen Substitutionen

$$(5) \qquad \begin{pmatrix} a, & b \\ 0, & a^{-1} \end{pmatrix} \pmod 7$$

bestehende, und wir wollen die Transformation also so einrichten, dass χ in dieser Form auftritt. Dies erreichen wir durch Transformation der Substitutionen (4) mittelst $\begin{pmatrix} 1, & 1 \\ -1, & 0 \end{pmatrix}$, und dadurch ergiebt sich aus (4)

$$(6) \qquad \chi = \begin{pmatrix} 2, & 3 \\ 0, & -3 \end{pmatrix}, \quad \omega = \begin{pmatrix} 1, & -3 \\ 3, & -1 \end{pmatrix}, \quad \Theta = \begin{pmatrix} 1, & 3 \\ -2, & 2 \end{pmatrix}.$$

Wir stellen hiernach noch zur besseren Uebersicht die ganze Octaëdergruppe in eine Tafel zusammen, deren sechs Zeilen die Elemente Θ^λ, $\omega\Theta^\lambda$, $\chi\Theta^\lambda$, $\chi\omega\Theta^\lambda$, $\chi^2\Theta^\lambda$, $\chi^2\omega\Theta^\lambda$ für $\lambda = 0, 1, 2, 3$ enthalten:

$$(7) \qquad \begin{array}{l}
\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \begin{pmatrix} 1, & 3 \\ -2, & 2 \end{pmatrix}, \begin{pmatrix} 2, & 2 \\ 1, & -2 \end{pmatrix}, \begin{pmatrix} 2, & -3 \\ 2, & 1 \end{pmatrix}; \\
\begin{pmatrix} 1, & -3 \\ 3, & -1 \end{pmatrix}, \begin{pmatrix} 0, & 3 \\ 2, & 0 \end{pmatrix}, \begin{pmatrix} -1, & 1 \\ -2, & 1 \end{pmatrix}, \begin{pmatrix} 3, & 1 \\ -3, & -3 \end{pmatrix}; \\
\begin{pmatrix} 2, & 3 \\ 0, & -3 \end{pmatrix}, \begin{pmatrix} 3, & -2 \\ -1, & 1 \end{pmatrix}, \begin{pmatrix} 0, & 2 \\ 3, & 1 \end{pmatrix}, \begin{pmatrix} 3, & -3 \\ 1, & -3 \end{pmatrix}; \\
\begin{pmatrix} 3, & 2 \\ 2, & -3 \end{pmatrix}, \begin{pmatrix} 1, & 1 \\ -1, & 0 \end{pmatrix}, \begin{pmatrix} 1, & 2 \\ 1, & 3 \end{pmatrix}, \begin{pmatrix} -3, & 0 \\ 2, & 2 \end{pmatrix}; \\
\begin{pmatrix} 3, & 3 \\ 0, & -2 \end{pmatrix}, \begin{pmatrix} -3, & 1 \\ -3, & 3 \end{pmatrix}, \begin{pmatrix} 2, & 0 \\ -2, & -3 \end{pmatrix}, \begin{pmatrix} -2, & 1 \\ 3, & -2 \end{pmatrix}; \\
\begin{pmatrix} -2, & 2 \\ 1, & 2 \end{pmatrix}, \begin{pmatrix} -1, & 2 \\ 3, & 0 \end{pmatrix}, \begin{pmatrix} 2, & 1 \\ 3, & 2 \end{pmatrix}, \begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix}.
\end{array}$$

Um die ganze Gruppe L_7 zu erhalten, müssen wir noch ein Element 7ten Grades hinzufügen, und dafür wählen wir

$$(8) \qquad \tau = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}.$$

Dann ist die gesammte Gruppe L_7 so dargestellt:

$$(9) \qquad \tau^\varrho \chi^\lambda \omega^\mu \Theta^\nu, \qquad \begin{array}{l} \varrho = 0, 1, 2, 3, 4, 5, 6 \\ \lambda = 0, 1, 2; \ \mu = 0, 1 \\ \nu = 0, 1, 2, 3. \end{array}$$

Dass alle diese Elemente (9) von einander verschieden sind, ergiebt sich einfach daraus, dass keine Potenz von τ, deren Exponent nicht durch 7 theilbar ist, in der Octaëdergruppe enthalten sein kann, weil die Octaëdergruppe kein Element vom 7ten Grade hat.

Die in der Gruppe L_7 enthaltene Gruppe (5) vom 21sten Grade ist dann in der Form $\tau^\varrho \chi^\lambda$ dargestellt.

Um die Composition der Elemente (9) zu charakterisiren, genügt es offenbar, wenn für jedes ϱ die Elemente

$$(10) \qquad \Theta \tau^\varrho, \quad \omega \tau^\varrho, \quad \chi \tau^\varrho$$

in der Form (9) dargestellt sind, weil dadurch, zusammen mit den Compositionen in der Octaëdergruppe, das symbolische Product je zweier Elemente der Form (9) wieder in der Form (9) dargestellt werden kann.

Da nun

$$(11) \qquad \tau^\varrho = \begin{pmatrix} 1, & \varrho \\ 0, & 1 \end{pmatrix}$$

ist, so erhält man zunächst sehr einfach aus (6)

$$(12) \qquad \chi \tau^\varrho = \tau^{4\varrho} \chi,$$

und daraus

$$(13) \qquad \chi^2 \tau^\varrho = \tau^{2\varrho} \chi^2,$$

und man sieht leicht, dass diese sechs Relationen eine Folge von der einen sind:

$$(14) \qquad \chi \tau = \tau^4 \chi.$$

Die übrigen Compositionen (10) erhält man aber nur durch wirkliche Ausrechnung in den einzelnen Fällen, wobei die Tabelle (7) gute Dienste leistet. Man wendet sie in der Weise an, dass man für jeden Werth ϱ die Elemente

$$\tau^{\varrho'} \omega \tau^\varrho, \quad \tau^{\varrho'} \Theta \tau^\varrho$$

bildet, und ϱ' so bestimmt, dass sich diese Elemente in der Tabelle finden, was immer nur auf eine Art möglich ist.

Man findet so durch leichte, wenn auch etwas umständliche Rechnung

$$(15)\qquad \begin{aligned} \omega\tau &= \tau^2\chi^2\omega\Theta^2, & \Theta\tau &= \tau^3\omega\Theta \\ \omega\tau^2 &= \tau\chi^2\Theta^3, & \Theta\tau^2 &= \tau\chi\omega\Theta^3 \\ \omega\tau^3 &= \tau^5\chi\Theta^2, & \Theta\tau^3 &= \tau^5\chi\omega \\ \omega\tau^4 &= \tau^4\chi^2\Theta, & \Theta\tau^4 &= \tau^6\omega\Theta^2 \\ \omega\tau^5 &= \tau^3\chi^2\omega\Theta, & \Theta\tau^5 &= \tau^2\Theta^3 \\ \omega\tau^6 &= \tau^6\omega\Theta^3, & \Theta\tau^6 &= \tau^4\chi^2\Theta^2. \end{aligned}$$

Diese zwölf Relationen lassen sich aber alle aus vieren von ihnen, die man auf mannigfaltige Art auswählen kann, als Folgerungen ableiten. Man kann z. B. für diese vier fundamentalen Relationen die folgenden wählen:

$$(16)\qquad \omega\tau = \tau^2\chi^2\omega\Theta^2,\quad \omega\tau^3 = \tau^5\chi\Theta^2,\quad \omega\tau^4 = \tau^4\chi^2\Theta,$$
$$\Theta\tau = \tau^3\omega\Theta,$$

aus denen mit Benutzung der Formeln (3), (12), (13) alle anderen leicht folgen, z. B.:

$$\omega\tau^5 = \tau^4\chi^2\Theta\tau = \tau^4\chi^2\tau^3\omega\Theta = \tau^3\chi^2\omega\Theta,$$

und so die übrigen.

Wie wir früher gesehen haben, dass wir als erzeugende Elemente der Octaëdergruppe χ und Θ betrachten können, so können wir jetzt als Erzeugende der Gruppe L_7 die zwei Elemente ω, τ ansehen, denn es ergiebt sich aus (15):

$$(17)\qquad \Theta^3 = \omega\tau\omega\tau^6,\quad \chi = \tau^2\Theta\tau^3\omega.$$

Fassen wir zusammen, so ergiebt sich folgendes Resultat:

I. Sind vier Elemente τ, χ, ω, Θ der Grade 7, 3, 2, 4 gegeben, bei deren Zusammensetzung die Relationen bestehen:

$$\begin{aligned} \omega\chi &= \chi^2\omega, & \Theta\omega &= \omega\Theta^3, & \Theta\chi &= \chi^2\omega\Theta^2, \\ \Theta^2\chi &= \chi\omega\Theta^3, & \omega\tau &= \tau^2\chi^2\omega\Theta^2, & \omega\tau^3 &= \tau^5\chi\Theta^2, \\ \omega\tau^4 &= \tau^4\chi^2\Theta, & \Theta\tau &= \tau^3\omega\Theta, & \chi\tau &= \tau^4\chi, \end{aligned}$$

so bilden die 168 Elemente

$$\sigma = \tau^\varrho\chi^\lambda\omega^\mu\Theta^\nu,$$

wenn ϱ, λ, μ, ν volle Restsysteme nach den Moduln 7, 3, 2, 4 durchlaufen, eine einfache Gruppe 168sten Grades, und ω und τ können als erzeugende Elemente dieser Gruppe angesehen werden.

Unter den Theilern dieser Gruppe sind hervorzuheben die Octaëdergruppe

$$\chi^\lambda \omega^u \Theta^v$$

vom Index 7, sodann die Elemente

$$\tau^\varrho \chi^\lambda,$$

die nach den Relationen (12) und (13) eine Gruppe 21sten Grades, also einen Theiler der Gesammtgruppe vom Index 8 bilden; ferner die Gruppe 8ten Grades $\omega^u \Theta^v$. Die gesammte Gruppe lässt sich auch in anderer Reihenfolge so darstellen:

$$\chi^\lambda \omega^u \Theta^v \tau^\varrho, \quad \omega^u \Theta^v \chi^\lambda \tau^\varrho, \quad \tau^\varrho \omega^u \Theta^v \chi^\lambda.$$

DRITTES BUCH.

ANWENDUNGEN

DER

GRUPPENTHEORIE.

Zehnter Abschnitt.

Allgemeine Theorie der metacyklischen Gleichungen.

---

§. 73.

Die Resolventen der Compositionsreihe.

Aus den Sätzen der allgemeinen Gruppentheorie, die im ersten Buche dieses Bandes behandelt sind, ergeben sich wichtige algebraische Folgerungen, wenn man sie auf die Galois'sche Gruppe einer Gleichung anwendet.

Es wird jetzt ein beliebiger Körper Ω als Rationalitätsbereich angenommen, $f(x) = 0$ sei eine Gleichung in diesem Körper ohne mehrfache Wurzeln und P ihre Galois'sche Gruppe. Diese Gruppe P habe einen Normaltheiler Q. Wir bezeichnen mit n den Grad von P und mit j den Index des Theilers Q, so dass $n:j$ der Grad von Q ist.

Wir haben im ersten Bande (§. 156) gesehen, dass die Gruppe von $f(x)$ durch Adjunction einer Wurzel einer irreduciblen Normalgleichung j^{ten} Grades auf Q reducirt wird und diese Hülfsgleichung j^{ten} Grades haben wir als Partialresolvente bezeichnet.

Die Galois'sche Gruppe dieser Partialresolvente haben wir so erhalten: Bedeutet ψ eine zu der Gruppe Q gehörige Function der Wurzeln von $f(x)$ und ist P in die Nebengruppen

$$P = Q + Qa + Qb + Qc + \cdots$$

zerlegt, wo also $a, b, c, \ldots$ gewisse Permutationen aus P sind, so geht ψ durch die ganze Nebengruppe Qa in ein und dieselbe Function ψ_a über, und die Galois'sche Gruppe der Resolvente besteht aus den Substitutionen

$$(\psi, \psi),\ (\psi, \psi_a),\ (\psi, \psi_b),\ (\psi, \psi_c), \ldots$$

Setzt man zwei dieser Substitutionen zusammen, so hat man zu beachten, dass

$$(\psi, \psi_b) = (\psi_a, \psi_{ab})$$

ist, so dass man

$$(\psi, \psi_a)\,(\psi, \psi_b) = (\psi, \psi_{ab})$$

hat. Es setzen sich also diese Substitutionen ganz in derselben Weise zusammen, wie nach §. 4 dieses Bandes die Nebengruppen, und es ergiebt sich daraus:

1. Die Galois'sche Gruppe der zu Q gehörigen Partialresolvente ist isomorph mit der zu Q complementären Gruppe P/Q.

Nehmen wir jetzt irgend eine Compositionsreihe von P mit der zugehörigen Indexreihe (§. 6):

$$(1)\qquad \begin{array}{c} P,\ P_1,\ P_2,\ \ldots,\ P_{\mu-1},\ 1 \\ j_1,\ j_2,\ \ldots,\ j_{\mu-1},\ j_\mu, \end{array}$$

so wird nach dem soeben Gesagten die Gruppe der Gleichung $f = 0$ von P auf P_1 reducirt durch Adjunction **einer** Wurzel einer Normalgleichung vom Grade j_1. Dann wird sie auf P_2 reducirt durch eine Wurzel einer Normalgleichung vom Grade j_2 u. s. f. und endlich wird die Gleichung vollständig gelöst durch eine Wurzel einer Normalgleichung vom Grade j_μ.

Auf dies Auflösungsverfahren fällt nun von dem Satze über die Unveränderlichkeit der Indexreihe (§. 6, I.) ein neues Licht.

2. Um die Gleichung $f = 0$ zu lösen, hat man nach einander je eine Wurzel einer Normalgleichung der Grade $j_1, j_2, \ldots, j_\mu$ zu adjungiren. Die Grade dieser Resolventen können zwar in der Reihenfolge, nicht aber in der Gesammtheit abgeändert werden.

Die Zahlen $j_1, j_2, \ldots, j_\mu$ hängen also weit tiefer mit der Natur einer Gleichung oder allgemeiner mit den durch die Gleichung definirten Körpern zusammen, als etwa der Grad der Gleichung; denn während der Grad durch Transformation auf mannigfache Weise verändert werden kann, wenn man Functionen der Wurzeln als neue Unbekannte einführt, bleiben die Zahlen $j_1, j_2, \ldots, j_\mu$ immer erhalten und sind als wahre **Invarianten** des durch die Gleichung definirten Normalkörpers zu betrachten.

Zu diesen Invarianten gehört auch der Grad n der Gruppe P selbst, der durch die j so bestimmt ist:

(2) $$n = j_1 j_2 \ldots j_{\mu-1} j_\mu.$$

Denn nach der Bedeutung der Indices ist $n : j_1$ der Grad von P_1, $n : j_1 j_2$ der Grad von P_2 u. s. f., und da der letzte der Grade gleich 1 ist, so ergiebt sich die Formel (2).

Im Allgemeinen ist in einer Compositionsreihe von P jedes Glied Normaltheiler nur des nächst vorangehenden. Es können aber auch einzelne Glieder vorkommen, die auch noch von weiter vorangehenden Gliedern Normaltheiler sind. Besonders wichtig sind solche Glieder, die Normaltheiler von P selbst und also auch von allen ihnen vorangehenden Gliedern der Compositionsreihe sind. Wir wollen sehen, welche algebraische Consequenzen aus diesem Umstande zu ziehen sind.

Es sei P_ν ein Glied der Reihe (1), welches zugleich Normaltheiler von P ist. Der Index von P_ν in Bezug auf P ist $j_1 j_2 \ldots j_\nu$, und dies Product ist der Grad der Partialresolvente, durch die die Gruppe P auf P_ν reducirt wird, die wir mit $\chi(y) = 0$ bezeichnen wollen. Die Gruppe dieser Resolvente, die eine Normalgleichung ist, erhalten wir nach dem Satze 1. in der Form P/P_ν.

Wir können nun leicht eine Compositionsreihe für diese Gruppe nebst der zugehörigen Indexreihe finden, nämlich:

(3) $$\begin{array}{cccccc} P/P_\nu, & P_1/P_\nu, & P_2/P_\nu, & \ldots, & P_{\nu-1}/P_\nu, & 1 \\ & j_1, & j_2, & \ldots, & j_{\nu-1}, & j_\nu. \end{array}$$

Denn nach dem Satze 1., §. 6 ist P_1/P_ν ein Normaltheiler von P/P_ν vom Index j_1, und es ist ein grösster Normaltheiler, weil nach 2., §. 6 über P_1/P_ν kein Normaltheiler von P/P_ν stehen kann, wenn über P_1 kein Normaltheiler von P steht. Und ebenso kann man in Bezug auf die folgenden Glieder von (3) schliessen.

Daraus ziehen wir noch eine wichtige Folgerung. Wir haben schon im §. 7 gezeigt, dass sich, wenn Q irgend ein Normaltheiler von P ist, eine Compositionsreihe von P finden lässt, in der Q vorkommt. Ist nun R ein anderer Normaltheiler von P und zugleich ein Theiler von Q, so kann man die Compositionsreihe von P so einrichten, dass Q und R darin vorkommen.

Wir denken uns eine solche Compositionsreihe bestimmt:

(4) $$P,\ Q',\ Q'',\ \ldots,\ Q,\ \ldots,\ R.$$

Nach (3) können wir die Compositionsreihen der beiden Gruppen P/Q und P/R daraus herleiten, die wir so andeuten wollen:

(5) $$P/Q,\ Q'/Q,\ Q''/Q, \ldots,\ 1$$

(6) $$P/R,\ Q'/R,\ Q''/R, \ldots,\ Q/R \ldots$$

Nun ist der Index des Theilers Q'/Q von P/Q gleich dem Index des Theilers Q' von P, also auch gleich dem Index des Theilers Q'/R von P/R (§. 6, 1.), und Gleiches gilt von den folgenden Gliedern. Wir sprechen also den Satz aus:

3. Sind Q und R Normaltheiler von P, und ist R ein Theiler von Q, so ist die Indexreihe von P/Q ein Theil der Indexreihe von P/R..

Sind die Indices $j_1, j_2, \ldots, j_\nu$ lauter Primzahlen, so ist die Lösung der Resolvente $\chi(y) = 0$ auf die Lösung einer Kette von cyklischen Gleichungen der Grade $j_1, j_2, \ldots, j_\nu$ reducirbar; diese Resolvente ist also metacyklisch in dem Sinne, wie wir diesen Begriff im siebzehnten Abschnitte des ersten Bandes festgestellt haben, wonach die metacyklischen Gleichungen mit den sonst algebraisch lösbar genannten identisch sind.

Eine irreducible Gleichung $f(x) = 0$ ist metacyklisch, wenn die Indexreihe ihrer Gruppe aus lauter Primzahlen besteht. Wir haben an der erwähnten Stelle die Bedingungen für metacyklische Gleichungen von Primzahlgrad untersucht, und müssen jetzt diese Betrachtungen für den allgemeinen Fall durchführen, dass der Grad der Gleichung beliebig zusammengesetzt ist.

§. 74.

Metacyklische Gleichungen.

Wenn $f(x) = 0$ eine irreducible Gleichung m^{ten} Grades und P ihre Galois'sche Gruppe ist, so ist P transitiv. Eine Compositions- und Indexreihe für P sei

(1) $$\begin{array}{l} P,\ P_1,\ P_2, \ldots,\ P_{\mu-1},\ 1 \\ \quad j_1,\ j_2, \ldots,\ j_{\mu-1},\ j_\mu. \end{array}$$

Es wird, da die letzte Gruppe 1 intransitiv ist, in der Compositionsreihe einmal eine intransitive Gruppe auftreten, und es sei also P_λ die erste intransitive Gruppe der Reihe (1). Dann

sind auch alle folgenden Gruppen $P_{\lambda+1}, P_{\lambda+2}, \ldots$, die ja alle Theiler von P_λ sind, intransitiv.

Es ist nun an die Sätze 1., 2., 3. im §. 158 des ersten Bandes zu erinnern. Da P_λ ein Normaltheiler von $P_{\lambda-1}$ ist, so folgt aus jenen Sätzen, dass $P_{\lambda-1}$ imprimitiv ist, und wenn durch die nöthigen Adjunctionen die Gruppe von $f(x) = 0$ auf $P_{\lambda-1}$ reducirt ist, so wird durch weitere Adjunction einer Wurzel einer Normalgleichung vom Grade j_λ die Function $f(x)$ in mehrere irreducible Factoren

(2) $$f(x) = f_1(x) f_2(x) \ldots f_h(x)$$

zerfallen, die alle von gleichem Grade sind und deren Anzahl h ein Theiler von j_λ ist.

Bezeichnen wir mit m den Grad von $f(x)$, mit m_1 den Grad von $f_1(x)$, so ist

(3) $$m = h m_1.$$

Nach dem angeführten Satze 1. im §. 158, Bd. I haben die Gleichungen $f_1 = 0, f_2 = 0, \ldots, f_h = 0$ alle dieselbe Gruppe, die wir mit Q bezeichnen wollen. Sind $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{m_1-1}$ die Wurzeln von $f_1 = 0$, so erhalten wir die Gruppe Q, wenn wir die Permutationen der α sammeln, die durch P_λ hervorgerufen werden. Es handelt sich zunächst um das Verhältniss der Grade p_λ und q der beiden Gruppen P_λ und Q.

Es kann mehrere verschiedene Permutationen in P_λ geben, die dasselbe Element in Q erzeugen, die also dieselbe Permutation der α enthalten. Sind π_1, π_2 zwei verschiedene Permutationen aus P_λ, die unter den α dieselbe Permutation hervorrufen, so wird $\pi_2 \pi_1^{-1} = \pi_0$ eine Permutation sein, die die α in Ruhe lässt, und es ist also $\pi_2 = \pi_0 \pi_1$. Wenn umgekehrt π_0 irgend eine Permutation aus P_λ ist, die die Wurzeln α nicht permutirt, so wird die Permutation $\pi_2 = \pi_0 \pi_1$ dieselbe Aenderung unter den α bedingen, wie π_1.

Es folgt hieraus, dass jede Permutation der α gleich oft durch die Permutationen von P_λ erzeugt wird, nämlich ebenso oft, als die α durch Permutationen aus P_λ ungeändert bleiben. Bezeichnen wir diese Zahl mit p_0, so ist also

(4) $$p_\lambda = p_0 q,$$

oder der Grad p_λ der Gruppe P_λ ist ein Vielfaches des Grades q von Q.

Wir haben nun im §. 154, 7. des ersten Bandes den Satz bewiesen, dass der Grad einer transitiven Permutationsgruppe immer durch die Anzahl der permutirten Ziffern theilbar ist. Hier ist aber $f_1(x)$ irreducibel und demnach die Gruppe Q transitiv. Es ist also q durch den Grad von $f_1(x)$, d. h. durch m_1 theilbar, und folglich ist nach (4) auch p_λ durch m_1 theilbar.

Den Grad $p_{\lambda-1}$ von $P_{\lambda-1}$ erhalten wir nach der Bedeutung von j_λ in der Form:

(5) $$p_{\lambda-1} = j_\lambda p_\lambda.$$

Nun ist p_λ ein Vielfaches von m_1, j_λ ein Vielfaches von h, und $h m_1 = m$ gleich dem Grade von $f(x)$. Demnach ist

(6) $$p_{\lambda-1} = k m$$

ein Vielfaches von m.

Aus der Bedeutung der j ergiebt sich aber [§. 73, (2)] $p_{\lambda-1} = j_\lambda j_{\lambda-1} \dots j_\mu$, und folglich haben wir die Relation

(7) $$j_\lambda j_{\lambda+1} j_{\lambda+2} \dots j_\mu = k m,$$

woraus sich eine sehr merkwürdige Folgerung ziehen lässt.

Angenommen, es werde die irreducible Function $f(x)$ durch successive Adjunction von Wurzeln cyklischer Gleichungen reducibel, dann lässt sich nach §. 176, Bd. I die Compositionsreihe (1) so geordnet annehmen, dass die Indices $j_1, j_2, \dots, j_\lambda$ Primzahlen sind. Es ist also, da h ein Theiler von j_λ ist, $j_\lambda = h$, und j_λ ist nach (3) eine in m aufgehende Primzahl.

Wenn nun in m ausser j_λ noch eine zweite Primzahl p aufgeht, so muss nach (7) einer der Factoren $j_\lambda, j_{\lambda+1}, j_{\lambda+2}, \dots, j_\mu$ durch p theilbar sein, und sie können also gewiss nicht alle gleich j_λ sein.

Daraus aber folgt nach dem Satze III, §. 7, dass man eine Compositionsreihe von P_λ:

(8) $$P_\lambda, P_{\lambda+1}, \dots, P_{\mu-1}, 1$$

so finden kann, dass unter den Gruppen $P_\lambda, P_{\lambda+1}, \dots, P_{\mu-1}$ eine, etwa P_ν, ein Normaltheiler von P ist.

Dieses P_ν ist aber als Theiler der intransitiven Gruppe P_λ selbst intransitiv, und daher muss P selbst **imprimitiv** sein (Bd. I, §. 158, 2).

Wir sprechen dies in folgender Form als Satz aus:

1. **Wenn im Grade einer irreduciblen Gleichung mehrere verschiedene Primzahlen aufgehen, so**

kann diese Gleichung nur dann durch successive Adjunction von Wurzeln cyklischer Gleichungen reducibel werden, wenn sie imprimitiv ist.

Wir können über die Art und Weise der Reduction, ihre Möglichkeit vorausgesetzt, noch einiges Nähere anführen. Ist P_ν die erste Gruppe der Reihe (8), die Normaltheiler von P ist, so ist nach dem eben angeführten Satze III, §. 7 bei richtiger Anordnung der Compositionsreihe:

$$(9) \qquad j_\lambda = j_{\lambda+1} \cdots = j_{\nu+1},$$

also alle gleich derselben Primzahl, und die Resolvente $\chi = 0$, durch die die Gruppe P auf P_ν reducirt wird, hat folglich eine metacyklische Gruppe.

Bezeichnen wir mit $A, B, \ldots, S$ die Systeme der Intransitivität der Gruppe P_ν, deren Anzahl s sei, und setzen

$$(10) \qquad m = r s,$$

so wird durch Adjunction einer Wurzel von $\chi = 0$ die Function $f(x)$ in s Factoren r^{ten} Grades zerfallen.

Die $A, B, \ldots, S$ sind Systeme der Imprimitivität von P (Bd. I, §. 158, 2.).

Bezeichnen wir mit Q die Gesammtheit aller Permutationen von P, die die einzelnen Systeme $A, B, \ldots, S$ an ihrer Stelle lassen und nur die Elemente der Systeme unter sich vertauschen, so ist Q, wie wir im §. 158 des ersten Bandes gesehen haben, ein Normaltheiler von P, und durch Adjunction der Wurzeln einer Hülfsgleichung s^{ten} Grades $\varphi(y) = 0$ zerfällt $f(x)$ in s Factoren r^{ten} Grades, denen die einzelnen Systeme $A, B, \ldots, S$ als Wurzeln angehören:

$$f(x) = f(x, y_\alpha)\, f(x, y_\beta)\, f(x, y_\gamma) \ldots$$

Da durch die Hülfsgleichung $\varphi(y) = 0$ die Gruppe P auf Q reducirt wird, so ist die Gruppe von $\varphi(y) = 0$ isomorph mit P/Q. Andererseits ist aber auch die intransitive Gruppe P_ν ein Theiler von Q, da die Systeme $A, B, \ldots, S$ durch P_ν nicht verschoben werden, und wir können also den Satz §. 73, 3. auf die drei Gruppen P, Q, P_ν anwenden. Da die Indexreihe von P/P_ν nach Voraussetzung aus lauter Primzahlen besteht, so gilt nach jenem Satze dasselbe von P/Q. Diese Gruppe ist metacyklisch und also ist auch die Hülfsgleichung $\varphi(y) = 0$ metacyklisch. Es folgt also der Satz:

2. **Wenn eine irreducible Gleichung, in deren Grad mehr als eine Primzahl aufgeht, durch successive Adjunction von Radicalen in Factoren zerfällt, so wird eine Zerfällung in s Factoren r^{ten} Grades herbeigeführt durch Adjunction der Wurzeln einer metacyklischen Gleichung r^{ten} Grades.**

Dieser Satz enthält als speciellen Fall den von **Abel** herrührenden Satz, dass eine irreducible Gleichung, deren Grad m nicht die Potenz einer Primzahl ist, nur dann durch Radicale lösbar sein kann, wenn sie durch Adjunction der Wurzeln einer lösbaren Gleichung niedrigeren Grades, deren Grad ein Theiler von m ist, in Factoren zerfällt [1]. Damit ist die Frage nach der Auflösung einer Gleichung durch Radicale oder auch nur der Reduction einer Gleichung durch Radicale ausserordentlich vereinfacht. Man kann in der That die fernere Untersuchung auf Gleichungen beschränken, deren Grad eine Primzahl oder eine Primzahlpotenz ist, weil darauf alle anderen Fälle durch wiederholte Anwendung des Satzes 2. zurückgeführt sind.

So gestattet z. B. die Frage nach allen durch Radicale lösbaren irreduciblen Gleichungen 6ten Grades eine geradezu triviale Antwort:

Um alle metacyklischen Gleichungen 6ten Grades in irgend einem Körper Ω zu erhalten, adjungire man dem Körper Ω eine Quadratwurzel und bilde in dem erweiterten Körper alle cubischen Gleichungen, oder man adjungire die Wurzel einer cubischen Gleichung und bilde in dem erweiterten Körper alle quadratischen Gleichungen.

Als Beispiel einer solchen Gleichung führen wir die von **Hesse** behandelte an, von der die Kreisschnitte einer nicht auf die Hauptaxen bezogenen Fläche 2ten Grades abhängen. Dies Problem wird durch Quadratwurzeln gelöst, wenn vorher durch die Lösung einer cubischen Gleichung die Hauptaxen bestimmt sind [2].

---

[1]) Abel giebt den Satz ohne Beweis in der Abhandlung „Sur la rés. algébr. des équations". Oeuvres complètes 1881, Bd. II, S. 217. Vgl. auch die Abhandlung von Galois in Liouville's Journal, Bd. 11.

[2]) Hesse, „Ueber die Auflösung derjenigen Gleichungen 6ten Grades etc." Crelle's Journal, Bd. 41 (1851).

§. 75.

Metacyklische Gleichungen, deren Grad eine Primzahlpotenz ist.

Nach den letzten Sätzen concentrirt sich das Interesse weiterer Untersuchungen über metacyklische Gleichungen hauptsächlich auf den Fall, dass der Grad der Gleichung eine Potenz p^k einer Primzahl p ist. Wir setzen die Gleichung als irreducibel voraus und beschränken uns auf die Betrachtung primitiver Gleichungen; denn die Auflösung der imprimitiven reducirt sich auf die successive Lösung zweier (oder mehrerer) primitiver Gleichungen, deren Grade gleichfalls Potenzen von p sind, und die, wenn die ursprüngliche Gleichung metacyklisch ist, auch metacyklisch sein müssen.

Wir nehmen also jetzt an, es sei P die Gruppe einer irreduciblen primitiven metacyklischen Gleichung $f(x) = 0$ vom Grade p^k. Nach Bd. I, §. 158, 2. muss nicht nur P selbst, sondern alle seine Normaltheiler (mit Ausnahme der Einheitsgruppe) noch transitiv sein. Nun wenden wir den in §. 8 allgemein bewiesenen Satz IV. an, nach dem P einen Normaltheiler Q mit lauter commutativen Elementen besitzt, und wenn mehrere solche Theiler vorhanden sind, so verstehen wir unter Q einen von ihnen, dessen Grad möglichst niedrig, aber noch grösser als 1 ist. Diese Gruppe Q ist also gleichfalls noch transitiv. Q kann aber keinen von der Einheit verschiedenen echten Theiler mehr haben, der zugleich Normaltheiler von P ist, weil sonst dieser an die Stelle von Q treten würde.

Wenn durch die gehörigen Adjunctionen die Gruppe unserer Gleichung von P auf Q reducirt ist, so ist $f(x) = 0$ in dem erweiterten Rationalitätsbereiche zu einer Abel'schen Gleichung geworden, und da sie noch irreducibel geblieben ist, so ist nach Bd. I, §. 162 der Grad der Gleichung gleich dem Grade der Gruppe; d. h. Q ist eine Abel'sche Gruppe vom Grade p^k. Die Grade aller Elemente von Q sind also Potenzen von p. Wir wollen nachweisen, dass ausser dem Einheitselemente in Q nur Elemente vom Grade p selbst vorkommen.

Nehmen wir an, es sei p^λ der höchste Grad, der unter den Elementen von Q vorkommt, und es sei $\lambda > 1$. Dann bilden alle Elemente von Q, deren Grad ein Theiler von $p^{\lambda-1}$ ist, einen

Theiler Q' von Q, der sowohl von Q selbst als von der Einheitsgruppe verschieden ist. Dieser Theiler Q' muss aber ein Normaltheiler von P sein, weil, wenn π in Q, γ in P enthalten ist, $\gamma^{-1}\pi\gamma$, was vom selben Grade wie π ist, gleichfalls in Q enthalten sein muss, und also zu Q' gehört, wenn π zu Q' gehört. Da nun aber, wie oben bemerkt, Q keinen echten Theiler haben kann, der grösser als die Einheitsgruppe und zugleich Normaltheiler von P ist, so muss $\lambda = 1$ sein.

§. 76.

Darstellung der Abel'schen Gruppe Q.

Die Betrachtungen des vorigen Paragraphen haben gezeigt, dass in einer metacyklischen Gruppe P, die als Galois'sche Gruppe einer irreduciblen primitiven Gleichung $f(x) = 0$ des Grades $n = p^k$ auftreten kann, eine Abel'sche Gruppe Q als Normaltheiler enthalten sein muss, deren Grad p^k ist, und die ausser dem Einheitselemente nur Elemente vom Grade p enthält.

Nach §. 9 lässt sich diese Gruppe Q durch eine Basis darstellen, die aus k Elementen $A_1, A_2, \ldots, A_k$ vom Grade p besteht, so dass jedes Element von Q die Form erhält:

(1) $$A_1^{z_1} A_2^{z_2} \ldots A_k^{z_k},$$

und hierin durchlaufen $z_1, z_2, \ldots, z_k$ von einander unabhängig je ein volles Restsystem nach dem Modul p. Wir gehen nun, um die entsprechende Permutationsgruppe zu finden, von einer beliebigen Wurzel x von $f(x)$ aus, bezeichnen die Wurzel, in die x durch die Permutation (1) übergeht, mit

(2) $$[z_1, z_2, \ldots, z_k],$$

und setzen fest, dass dies Zeichen seine Bedeutung nicht ändern soll, wenn die Zahlen $z_1, z_2, \ldots, z_k$ beliebig um Vielfache von p verändert werden. Der Wurzel x, von der wir ausgingen, kommt dann das Zeichen $[0, 0, \ldots, 0]$ zu, und durch das Zeichen (2) ist jede Wurzel von $f(x)$ ein und nur einmal dargestellt.

Wenn x durch eine Permutation A' in x' und x' durch A'' in x'' übergeht, so geht x durch die Permutation $A' A''$ in x'' über. Daraus folgt aber, dass $[z_1, z_2, \ldots, z_k]$ durch die Permutation

(3) $$A = A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_k^{\alpha_k}$$

in $[z_1 + \alpha_1, z_2 + \alpha_2, \ldots, z_k + \alpha_k]$ übergeht. Demnach können wir die Permutation A auch so bezeichnen:

$$(4) \qquad \begin{pmatrix} z_1, & z_2, & \ldots, & z_k \\ z_1 + \alpha_1, & z_2 + \alpha_2, & \ldots, & z_k + \alpha_k \end{pmatrix},$$

und man erhält die ganze Gruppe Q, wenn man $\alpha_1, \alpha_2, \ldots, \alpha_k$ je ein volles Restsystem nach dem Modul p durchlaufen lässt.

Die Gruppe Q, deren Bildungsweise jetzt festgestellt ist, muss ein Normaltheiler von P sein, und daraus lässt sich eine allgemeine Form herleiten, in der alle Permutationen von P enthalten sein müssen.

Dazu bedürfen wir eines Hülfssatzes über die analytische Darstellung der Permutationen, den wir zunächst ableiten.

§. 77.

Analytische Darstellung der Permutationen.

Hülfssatz. Wenn bei irgend einer Permutation der Grössen (2), §. 76, z_1 in z'_1, z_2 in $z'_2, \ldots, z_k$ in z'_k übergeht, so kann man immer

$$(1) \qquad \left.\begin{aligned} z'_1 &\equiv \varphi_1 (z_1, z_2, \ldots, z_k) \\ z'_2 &\equiv \varphi_2 (z_1, z_2, \ldots, z_k) \\ &\ldots\ldots\ldots\ldots \\ z'_k &\equiv \varphi_k (z_1, z_2, \ldots; z_k) \end{aligned}\right\} \pmod{p}.$$

setzen, worin $\varphi_1, \varphi_2, \ldots, \varphi_k$ ganze rationale Functionen der Variablen $z_1, z_2, \ldots, z_k$ mit ganzzahligen Coëfficienten bedeuten, die in Bezug auf keine der Variablen den Grad $p - 1$ übersteigen.

Der Satz ist eine Verallgemeinerung des entsprechenden Satzes im §. 180 des ersten Bandes. Dort ist der Satz für $k = 1$ bewiesen. Dem allgemeinen Beweise, der auf der vollständigen Induction beruht, schicken wir folgende Erwägungen voraus.

Da wir in (1) für die Argumente z_i alle Combinationen von k Reihen nach dem Modul p zu setzen haben, so ergeben sich p^k solcher Systeme. Jede der Functionen φ hat p^k unbestimmte Coëfficienten, und wenn also die z'_k gegeben sind, so erhalten wir kp^k lineare Congruenzen für ebenso viele unbekannte Zahlen, nämlich die Coëfficienten der φ_k. Es ist nur noch nachzuweisen,

dass diese Congruenzen von einander unabhängig sind. Hierbei können wir jede der Functionen φ für sich betrachten. Setzen wir also

(2) $$z' \equiv \varphi(z_1, z_2, \ldots, z_k) \pmod{p},$$

so haben wir, wenn wir für jede Combination der z_i den zugehörigen Werth von z' kennen, p^k lineare Congruenzen zur Bestimmung der Coëfficienten von φ. Es ist zu beweisen, dass diese Congruenzen immer lösbar sind, wobei wir voraussetzen können, dass diese Möglichkeit für Functionen von weniger Variablen schon erwiesen sei.

Wenn wir nun φ nach Potenzen der Variablen z_1 ordnen, so erhalten wir

(3) $$z' \equiv \chi_0 z_1^{p-1} + \chi_1 z_1^{p-2} + \cdots + \chi_{p-1} \pmod{p},$$

worin die Coëfficienten $\chi_0, \chi_1, \ldots, \chi_{p-1}$ ebensolche Functionen sind wie φ, nur dass sie von einer Variablen weniger abhängen.

Halten wir irgend eine der Combinationen der $z_2, \ldots, z_k$ fest, und setzen $z_1 = 0, 1, \ldots, p-1$, so erhalten wir aus (3) ein System von p linearen Congruenzen, dessen Determinante nicht durch p theilbar ist, und wir können daraus, wie im §. 180 des ersten Bandes, die Werthe von $\chi_0, \chi_1, \ldots, \chi_{p-1}$ für diese Combination der $z_2, \ldots, z_k$ bestimmen, und daher sind für jede Combination der Variablen die Werthe der Function χ_i (nach dem Modul p) bekannt. Der Voraussetzung nach können wir aber die Coëfficienten der Functionen χ_i, die ja nur von $k-1$ Variablen abhängen, daraus bestimmen, und damit ist der Hülfssatz bewiesen.

Hiernach können wir jede Permutation der Wurzeln $[z_1, \ldots, z_k]$ so darstellen:

(4) $$\begin{pmatrix} z_1, & z_2, \ldots \\ \varphi_1(z_1, z_2, \ldots), & \varphi_2(z_1, z_2, \ldots), \ldots \end{pmatrix},$$

oder in noch abgekürzterer Schreibweise:

(5) $$\begin{pmatrix} z \\ \varphi(z) \end{pmatrix}.$$

In dem Symbol (4) können wir, ohne seine Bedeutung zu ändern, $z_1, z_2, \ldots$ durch irgend eine andere Combination $z_1', z_2', \ldots$ ersetzen, und wenn also nach dem Hülfssatze

$$z_i' = \psi_i(z_1, z_2, \ldots)$$

ist, so können wir (4) oder (5) auch so darstellen:

$$(6)\qquad \begin{pmatrix}\psi_1(z_1, z_2, \ldots), & \psi_2(z_1, z_2, \ldots), \ldots \\ \varphi_1(\psi_1, \psi_2, \ldots), & \varphi_2(\psi_1, \psi_2, \ldots), \ldots\end{pmatrix} = \begin{pmatrix}\psi(z) \\ \varphi\,[\psi(z)]\end{pmatrix}.$$

Dies führt zur Zusammensetzung der Permutationen:

$$(7)\qquad \begin{pmatrix}z \\ \psi(z)\end{pmatrix}\begin{pmatrix}z \\ \varphi(z)\end{pmatrix} = \begin{pmatrix}z \\ \varphi\,[\psi(z)]\end{pmatrix}.$$

§. 78.

Darstellung der metacyklischen Gruppe *P*.

Nun soll die Gruppe Q ein Normaltheiler der Gruppe P sein, d. h. wenn A eine Permutation aus Q, B eine Permutation aus P ist, so soll sich eine zweite Permutation A' aus Q so bestimmen lassen, dass

$$(1)\qquad AB = BA'$$

ist. Setzen wir in der abgekürzten Bezeichnung des vorigen Paragraphen

$$A = \begin{pmatrix}z \\ z+\alpha\end{pmatrix},\quad A' = \begin{pmatrix}z \\ z+\alpha'\end{pmatrix},\quad B = \begin{pmatrix}z \\ \varphi(z)\end{pmatrix},$$

so wird

$$AB = \begin{pmatrix}z \\ \varphi\,(z+\alpha)\end{pmatrix},\quad BA' = \begin{pmatrix}z \\ \varphi\,(z)+\alpha'\end{pmatrix},$$

oder

$$\varphi\,(z+\alpha) \equiv \varphi\,(z) + \alpha'.$$

Diese Congruenz aber ist nur ein abgekürztes Symbol für das System der Congruenzen nach dem Modul p:

$$(2)\qquad \begin{aligned} \varphi_1\,(z_1+\alpha_1, z_2+\alpha_2, \ldots) &\equiv \varphi_1\,(z_1, z_2, \ldots) + \alpha_1' \\ \varphi_2\,(z_1+\alpha_1, z_2+\alpha_2, \ldots) &\equiv \varphi_2\,(z_1, z_2, \ldots) + \alpha_2' \\ \cdots\cdots&\cdots\cdots \end{aligned}$$

Hierin kann das System der Zahlen $\alpha_1, \alpha_2, \ldots$ nach dem Modul p beliebig gegeben sein, $\alpha_1', \alpha_2', \ldots$ sind dadurch bestimmt.

Setzen wir in der ersten der Formeln (2) je eine der Zahlen $\alpha_1, \alpha_2, \ldots$ gleich 1, die übrigen gleich 0, so mag sich ergeben:

$$(3)\qquad \begin{aligned} \varphi_1\,(z_1+1, z_2 \ldots) &\equiv \varphi_1\,(z_1, z_2, \ldots) + \alpha_{1,1} \\ \varphi_1\,(z_1, z_2+1, \ldots) &\equiv \varphi_1\,(z_1, z_2, \ldots) + \alpha_{1,2} \\ \cdots\cdots&\cdots\cdots \end{aligned}$$

Wenn man die erste dieser Formeln α_1 mal, die zweite α_2 mal nach einander anwendet u. s. f., so folgt:

$$\varphi_1(z_1+\alpha_1, z_2, \ldots) \equiv \varphi_1(z_1, z_2, \ldots) + \alpha_1 \alpha_{1,1}$$
$$\varphi_1(z_1, z_2+\alpha_2, \ldots) \equiv \varphi_1(z_1, z_2, \ldots) + \alpha_2 \alpha_{1,2}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

und wenn man in der ersten z_2 in $z_2+\alpha_2$ verwandelt, und die zweite anwendet und so fortfährt, so ergiebt sich schliesslich:

$$(4) \qquad \varphi_1(z_1+\alpha_1, z_2+\alpha_2, \ldots) \equiv \varphi_1(z_1, z_2, \ldots) + \alpha_1 \alpha_{1,1} + \alpha_2 \alpha_{1,2} + \cdots$$

Hierin setzen wir nun $z_1, z_2, \cdots = 0$ und schreiben dann an Stelle von $\alpha_1, \alpha_2, \ldots$ wieder $z_1, z_2, \ldots$ Ferner bezeichnen wir $\varphi_1(0, 0, \ldots)$ durch α_1 und erhalten so aus (4):

$$(5) \qquad \varphi_1(z_1, z_2, \ldots) \equiv \alpha_1 + z_1\, \alpha_{1,1} + z_2\, \alpha_{1,2} + \cdots,$$

d. h. φ_1 muss eine lineare Function sein.

Genau auf dieselbe Weise verfahren wir mit sämmtlichen Congruenzen (2) und gelangen so zu folgendem Endresultate:

I. Alle Permutationen der Galois'schen Gruppe P einer primitiven irreduciblen metacyklischen Gleichung vom Grade p^k

$$\begin{pmatrix} z_1, & z_2, & \ldots, & z_k \\ z_1', & z_2', & \ldots, & z_k' \end{pmatrix}$$

sind von der Form

$$(6) \qquad \begin{array}{l} z_1' \equiv \alpha_{1,1} z_1 + \alpha_{1,2} z_2 + \cdots + \alpha_{1,k} z_k + \alpha_1 \\ z_2' \equiv \alpha_{2,1} z_1 + \alpha_{2,2} z_2 + \cdots + \alpha_{2,k} z_k + \alpha_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ z_k' \equiv \alpha_{k,1} z_1 + \alpha_{k,2} z_2 + \cdots + \alpha_{k,k} z_k + \alpha_k \end{array} \quad (\text{mod } p).$$

Das System der Congruenzen (6) stellt immer dann und nur dann eine Permutation dar, wenn die Determinante

$$\Sigma \pm \alpha_{1,1}\, \alpha_{2,2} \ldots \alpha_{k,k}$$

nicht durch p theilbar ist, weil dann und nur dann auch umgekehrt zu jedem Systeme der z' ein bestimmtes System der z (nach dem Modul p) gehört.

Der Inbegriff aller Permutationen (6) ist in der That eine Gruppe, die die allgemeine lineare Congruenzgruppe heisst, und in ihr müssen die metacyklischen Gruppen P ent-

halten sein. Es sind aber nicht alle linearen Congruenzgruppen auch umgekehrt metacyklisch, und diese daraus auszusondern, ist noch ein weiteres Problem, das bis jetzt nur in besonderen Fällen gelöst ist [1]).

Um aber das Problem wenigstens genauer zu formuliren, fügen wir noch folgende Betrachtungen bei.

Wir bezeichnen die vollständige lineare Congruenzgruppe (6) mit R, und sondern daraus die darin enthaltene Gruppe der linearen homogenen Substitutionen

$$
\begin{aligned}
z_1' &\equiv \alpha_{1,1} z_1 + \alpha_{1,2} z_2 + \cdots + \alpha_{1,k} z_k \\
z_2' &\equiv \alpha_{2,1} z_1 + \alpha_{2,2} z_2 + \cdots + \alpha_{2,k} z_k \\
&\cdots\cdots\cdots\cdots \\
z_k' &\equiv \alpha_{k,1} z_1 + \alpha_{k,2} z_2 + \cdots + \alpha_{k,k} z_k
\end{aligned}
\pmod p \tag{7}
$$

mit nicht verschwindender Determinante ab, die **lineare homogene Congruenzgruppe** genannt, die wir mit S bezeichnen wollen. Ferner ist in (6) die $k$fach cyklische Gruppe Q enthalten, die aus den Substitutionen

$$z_1' = z_1 + \alpha_1,\quad z_2' = z_2 + \alpha_2, \ldots, z_k' = z_k + \alpha_k \tag{8}$$

besteht.

Bedeutet nun σ ein Element aus S und γ ein Element aus Q, so ergiebt sich aus der Compositionsregel §. 77, (7) ohne Schwierigkeit, dass sich jede Substitution π aus der Gruppe R **auf eine und nur auf eine** Weise in jeder der beiden Formen

$$\pi = \sigma\gamma = \gamma'\sigma \tag{9}$$

darstellen lässt, worin, wenn σ, γ durch (7), (8) bestimmt sind, γ' die Substitution

$$z_1' = z_1 + \alpha_1',\quad z_2' = z_2 + \alpha_2', \ldots, z_k' = z_k + \alpha_k' \tag{10}$$

bedeutet, wenn die α_i' aus den α_i durch die Substitution σ abgeleitet sind.

Q ist ein Normaltheiler von R; denn ist γ_1 ein beliebiges Element aus Q, so ist bei mehrmaliger Anwendung von (9):

$$\sigma\gamma\gamma_1 = \gamma'\gamma_1'\sigma = \gamma'\gamma_1'\sigma\gamma^{-1}\gamma = \gamma'\gamma_1'\gamma'^{-1}\sigma\gamma,$$

also, wenn

$$\sigma\gamma = \pi,\quad \gamma'\gamma_1'\gamma'^{-1} = \gamma_1''$$

gesetzt wird,

$$\pi\gamma_1 = \gamma_1''\pi,$$

---

[1]) C. **Jordan**, Liouville's Journ. de Mathém. Sér. (2), Bd. XIII.

und folglich

(11) $$\pi^{-1} Q \pi = Q.$$

Wenn nun π irgend einen Theiler R_1 von R durchläuft, der seinerseits die Gruppe Q enthält, so ist Q Normaltheiler von R_1 und die in (9) vorkommende Substitution σ muss einen Theiler S_1 von S durchlaufen. Man kann setzen:

$$R_1 = S_1 Q = Q S_1,$$

und da die in der Form (9) enthaltenen Substitutionen alle von einander verschieden sind, so ist der Grad von R_1 gleich dem Producte der Grade von S_1 und Q. Ist R_2 ein Normaltheiler von R_1, der gleichfalls noch Q (als Normaltheiler) enthält, so ist ebenso

$$R_2 = S_2 Q,$$

und S_2 ist ein Normaltheiler von S_1.

Denn nach Voraussetzung ist für jedes Element π_1 aus R_1

$$\pi_1^{-1} S_2 Q \pi_1 = S_2 Q,$$

also nach (11):

$$\pi_1^{-1} S_2 Q \pi_1 = \pi_1^{-1} S_2 \pi_1 Q = S_2 Q,$$

und folglich

$$\pi_1^{-1} S_2 \pi_1 = S_2,$$

und da dies auch für $\pi_1 = \sigma_1$ gilt, wo σ_1 in S_1 enthalten ist, so ist S_2 Normaltheiler von S_1. Umgekehrt ist, wenn S_2 ein Normaltheiler von S_1 ist, $S_2 Q$ Normaltheiler von $S_1 Q$. Denn wenn $S_2 \sigma_1 = \sigma_1 S_2$ ist, so folgt

$$\sigma_1 S_2 Q = S_2 \sigma_1 Q = S_2 Q \sigma_1,$$

und daraus

$$\gamma \sigma_1 S_2 Q = \gamma S_2 Q \sigma_1 = S_2 \gamma' Q \sigma_1 = S_2 Q \sigma_1$$
$$= S_2 Q \gamma^{-1} \gamma \sigma_1 = S_2 Q \gamma \sigma_1$$

(weil $\gamma' Q = Q \gamma^{-1} = Q$ ist); d. h.

$$\pi_1 S_2 Q = S_2 Q \pi_1,$$

w. z. b. w. Hieraus aber ergiebt sich Folgendes:

II. Ist P die Galois'sche Gruppe einer primitiven irreduciblen metacyklischen Gleichung vom Grade p^k, so ist P in der Form darstellbar:

$$P = T Q,$$

worin T eine in der Congruenzgruppe S enthaltene metacyklische Gruppe ist.

Die Aufgabe der Auffindung aller dieser metacyklischen Gleichungen ist also darauf zurückgeführt, alle metacyklischen Theiler der homogenen Congruenzgruppe S zu finden.

Nehmen wir als Beispiel den Fall $p = 3$, $k = 2$, fragen also nach den metacyklischen Gleichungen 9ten Grades, so handelt es sich nach diesem Satze um die Gruppe S der nach dem Modul 3 genommenen linearen Substitutionen

(12) $$\sigma = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix},$$

mit denen wir uns, unter etwas anderem Gesichtspunkte, im §. 66 beschäftigt haben.

Wir haben dort zunächst einen Theiler E von S betrachtet, der aus allen Substitutionen σ mit der Bedingung $a\,d - b\,c \equiv 1 \pmod 3$ besteht, und haben ausserdem zwei Substitutionen

(13) $$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}, \begin{pmatrix} -a, & -b \\ -c, & -d \end{pmatrix}$$

zu einem einzigen Elemente zusammengefasst. Die so specialisirte Gruppe war vom Grade 12 und hatte einen Normaltheiler vom Index 3:

$$G = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \begin{pmatrix} -1, & 1 \\ 1, & 1 \end{pmatrix}, \begin{pmatrix} 1, & 1 \\ 1, & -1 \end{pmatrix},$$

aus dem E so zusammengesetzt war:

$$E = G + \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} G + \begin{pmatrix} 1, & 0 \\ -1, & 1 \end{pmatrix} G.$$

In der Gruppe S gelten aber die beiden Substitutionen (13) als verschieden, und ausserdem müssen noch die Substitutionen σ, deren Determinante $a\,d - b\,c \equiv -1 \pmod 3$ ist, dazu genommen werden, wodurch sich der Grad der Gruppe auf 48 erhöht. G erweitert sich durch die Aenderung der Vorzeichen aller Elemente zu einer Gruppe 8ten Grades und E zu einer Gruppe 24sten Grades, von der das erweiterte G Normaltheiler ist. Hier ist nun die ganze Gruppe S metacyklisch, wie man aus folgender Zusammensetzung sieht, in der die erweiterte Gruppe G mit S_2 und die erweiterte Gruppe E mit S_1 bezeichnet ist:

$$S_4 = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}$$

$$S_3 = S_4 + \begin{pmatrix} -1, 1 \\ 1, 1 \end{pmatrix} S_4$$

$$S_2 = S_3 + \begin{pmatrix} 0, 1 \\ -1, 0 \end{pmatrix} S_3$$

$$S_1 = S_2 + \begin{pmatrix} 1, 0 \\ 1, 1 \end{pmatrix} S_2 + \begin{pmatrix} 1, 0 \\ -1, 1 \end{pmatrix} S_2$$

$$S = S_1 + \begin{pmatrix} -1, 0 \\ 0, 1 \end{pmatrix} S_1.$$

Wir haben hiernach die Compositions- und Indexreihe von S

$$\begin{matrix} S, & S_1, & S_2, & S_3, & S_4, \\ & 2 & 3 & 2 & 2 \end{matrix}$$

und wir kommen also hier zu dem Ergebniss, dass alle Gleichungen 9ten Grades mit linearer Congruenzgruppe metacyklisch sind.

§. 79.

Ternäre lineare Congruenzgruppe für den Modul 2.

Mannigfache interessante Beziehungen ergeben sich, wenn wir die ternäre lineare Congruenzgruppe R für den Modul 2 betrachten, die als transitive Permutationsgruppe von acht Elementen aufgefasst werden kann, und die Gruppe der metacyklischen Gleichungen 8ten Grades enthalten muss. Nach dem oben Bewiesenen kommt es vor Allem darauf an, die homogene Congruenzgruppe S zu betrachten, die aus den Elementen

$$(1) \qquad \sigma = \begin{pmatrix} a\,, b\,, c \\ a_1, b_1, c_1 \\ a_2, b_2, c_2 \end{pmatrix}$$

besteht, worin die Ziffern $a, b, c, \ldots$ nach dem Modul 2, also $= 0$ oder $= 1$, anzunehmen sind, und die nach der im §. 37 gegebenen Vorschrift componirt werden. Es kommen dabei nur solche Systeme der Zahlen $a, b, c, \ldots$ in Betracht, deren Determinante $= 1$, d. h. ungerade ist.

Um den Grad der Gruppe S zu ermitteln, beachte man, dass die erste Zeile von σ sieben verschiedene Formen haben kann:

$$(1,0,0),\ (0,1,0),\ (0,0,1),\ (0,1,1),\ (1,0,1),\ (1,1,0),\ (1,1,1).$$

Für die erste Annahme $(a, b, c) = (1, 0, 0)$ wird die Determinante von σ gleich $b_1 c_2 - c_1 b_2$, was auf sechs verschiedene Arten $= 1$ werden kann, nämlich:

$$\begin{pmatrix} b_1, c_1 \\ b_2, c_2 \end{pmatrix} = \begin{pmatrix} 1, 0 \\ 0, 1 \end{pmatrix}, \begin{pmatrix} 1, 0 \\ 1, 1 \end{pmatrix}, \begin{pmatrix} 0, 1 \\ 1, 0 \end{pmatrix}, \begin{pmatrix} 0, 1 \\ 1, 1 \end{pmatrix}, \begin{pmatrix} 1, 1 \\ 1, 0 \end{pmatrix}, \begin{pmatrix} 1, 1 \\ 0, 1 \end{pmatrix}.$$

Dann können noch a_1, a_2 auf vier verschiedene Arten angenommen werden. Also hat man, wenn die erste Zeile $(1, 0, 0)$ ist, 24 verschiedene Formen von σ. Dieselbe Zahl ergiebt sich für die Annahme der ersten Zeile in den Formen $(0, 1, 0)$, $(0, 0, 1)$. Das Gleiche erhält man aber auch für die anderen Annahmen über die erste Zeile. Denn ist diese z. B. $(0, 1, 1)$, so muss

$$a_1 (b_2 - c_2) - a_2 (b_1 - c_1) \equiv 1 \pmod 2$$

sein, was wieder sechs Möglichkeiten für $a_1, b_1 - c_1, a_2, b_2 - c_2$ ergiebt, und da man c_1, c_2 auf vier Arten annehmen kann, so erhält man wieder 24 Möglichkeiten. Endlich muss, wenn die erste Zeile $(1, 1, 1)$ ist,

$$(a_1 - c_1)(b_2 - c_2) - (a_2 - c_2)(b_1 - c_1) \equiv 1 \pmod 2$$

sein, was zu derselben Zahl führt.

Die Gesammtzahl aller verschiedenen Substitutionen σ, d. h. der Grad von S ist also 168. Die Zahl 168 als Gradzahl einer Gruppe ist uns schon einmal begegnet, nämlich bei der Gruppe L_7 (§. 66, 72), und es liegt daher die Vermuthung nahe, dass die Gruppen S und L_7 isomorph sein möchten. Wenn sich diese Vermuthung bestätigt, so würde die Untersuchung der Gruppe S dadurch wesentlich erleichtert sein, dass wir die Divisoren der Gruppe L_7 schon kennen.

Diese Vermuthung zu prüfen, dient aber das Theorem I. in §. 72.

Wir suchen zu diesem Zweck erzeugende Elemente $\chi, \omega, \Theta, \tau$ der Gruppe S so auszuwählen, dass sie den charakteristischen Bedingungen des Theorems I., §. 72 genügen. Dies kann auf mehrfache Weise geschehen. Es fehlt freilich an einem allgemeinen Verfahren dazu, gelingt aber leicht durch einige Versuche.

Man wählt zunächst ein Element 7ten Grades beliebig aus und bildet daraus die Periode, etwa

(2)
$$\tau = \begin{pmatrix}1, 0, 1\\ 1, 0, 0\\ 0, 1, 0\end{pmatrix},\ \tau^2 = \begin{pmatrix}1, 1, 1\\ 1, 0, 1\\ 1, 0, 0\end{pmatrix},\ \tau^3 = \begin{pmatrix}0, 1, 1\\ 1, 1, 1\\ 1, 0, 1\end{pmatrix}$$
$$\tau^4 = \begin{pmatrix}1, 1, 0\\ 0, 1, 1\\ 1, 1, 1\end{pmatrix},\ \tau^5 = \begin{pmatrix}0, 0, 1\\ 1, 1, 0\\ 0, 1, 1\end{pmatrix},\ \tau^6 = \begin{pmatrix}0, 1, 0\\ 0, 0, 1\\ 1, 1, 0\end{pmatrix}.$$

Hierauf sucht man unter den Elementen 2ten Grades, deren es 21 giebt, ein passendes für ω aus; es eignet sich z. B. dieses

(3)
$$\omega = \begin{pmatrix}1, 0, 0\\ 0, 1, 0\\ 0, 1, 1\end{pmatrix};$$

und dann sind nach den Formeln §. 72, (17) die Elemente Θ und χ bestimmt:

(4)
$$\Theta = \begin{pmatrix}1, 1, 1\\ 0, 1, 0\\ 0, 1, 1\end{pmatrix},\ \Theta^2 = \begin{pmatrix}1, 1, 0\\ 0, 1, 0\\ 0, 0, 1\end{pmatrix},\ \Theta^3 = \begin{pmatrix}1, 0, 1\\ 0, 1, 0\\ 0, 1, 1\end{pmatrix}$$

(5)
$$\chi = \begin{pmatrix}1, 0, 0\\ 0, 0, 1\\ 0, 1, 1\end{pmatrix},\ \chi^2 = \begin{pmatrix}1, 0, 0\\ 0, 1, 1\\ 0, 1, 0\end{pmatrix}.$$

Hierauf ist es Sache einer einfachen Rechnung, die Formeln des Theorems I., §. 72 zu bestätigen, wodurch die Uebereinstimmung der Gruppen S und L_7 nachgewiesen ist.

Es folgt daraus, dass die Gruppe S ebenso wie L_7 einfach ist.

§. 80.

Resolventen der Gleichung 8ten Grades.

Um nun die Anwendung auf die Theorie der Gleichungen 8ten Grades zu machen, bezeichnen wir wie früher mit Q die cyklische Gruppe 8ten Grades:

$$\begin{pmatrix}z_1, & z_2, & z_3\\ z_1 + h_1, & z_2 + h_2, & z_3 + h_3\end{pmatrix} \pmod 2,$$

oder kürzer

$$(z_i,\ z_i + h_i),$$

und mit S die im §. 79 betrachtete ternäre Congruenzgruppe, und setzen

$$R = SQ,$$

so dass R die gesammte ternäre lineare Congruenzgruppe für den Modul 2 ist.

Wir betrachten ein System von acht unabhängigen Veränderlichen X_{z_1, z_2, z_3}, worin die Indices z_1, z_2, z_3 nach dem Modul 2 zu nehmen sind.

Hieraus bilden wir die sieben Functionen (Lagrange'sche Resolventen, Bd. I, §. 164).

$$(1) \qquad \sum^{z} (-1)^{\Sigma z \xi} X_{z_1, z_2, z_3} = \Psi_{\xi_1, \xi_2, \xi_3},$$

worin zur Abkürzung

$$\Sigma z \xi = z_1 \xi_1 + z_2 \xi_2 + z_3 \xi_3$$

gesetzt ist, und ξ_1, ξ_2, ξ_3 je ein volles Restsystem nach dem Modul 2, jedoch mit Ausschluss der Combination 0, 0, 0 durchlaufen.

Wenden wir auf die Indices z_i der Grössen X die Substitutionen der Gruppe Q an, so erleiden die X die Permutationen einer Gruppe, die wir gleichfalls mit Q bezeichnen. Die Aenderungen der Ψ, die diesen Permutationen entsprechen, ergeben sich aus (1), wenn wir auf die Indices der X die Substitution $(z_i, z_i + h)$ anwenden:

$$(2) \qquad \Sigma (-1)^{\Sigma z \xi} X_{z_1 + h_1, z_2 + h_2, z_3 + h_3} = \sum^{z} (-1)^{\Sigma (z + h) \xi} X_{z_1, z_2, z_3}$$
$$= (-1)^{\Sigma h \xi} \Psi_{\xi_1, \xi_2, \xi_3}.$$

1. Die Functionen Ψ ändern also durch die Permutationen von Q nur ihr Zeichen, und die Quadrate der Ψ bleiben durch Q ungeändert.

Es ist ferner der Einfluss einer Substitution σ aus S auf die Functionen Ψ festzustellen.

Bezeichnen wir zu diesem Zwecke mit ϱ die transponirte Substitution zu σ und setzen

$$(3) \qquad z' = \sigma(z), \quad \xi = \varrho(\xi'), \quad \xi' = \varrho^{-1}(\xi),$$

so ist (§. 37, 9.):

$$(4) \qquad \Sigma \xi z = \Sigma \xi' z'.$$

Machen wir die Substitutionen σ der Gruppe S in den Indices von X, so erhalten wir eine mit S zu bezeichnende Permutationsgruppe der X, und aus (1) ergiebt sich

$$\sum^{z} (-1)^{\Sigma z \xi} X_{z_1', z_2', z_3'} = \sum^{z} (-1)^{\Sigma \xi' z'} X_{z_1', z_2', z_3'},$$

und da das System der z'_i dieselbe Werthreihe durchläuft, wie das System der z_i, so ist diese Summe gleich $\Psi_{\xi_1', \xi_2', \xi_3'}$, und wir erhalten:

2. **Die Anwendung der Permutation σ auf die X in den Functionen Ψ ist gleichbedeutend mit der Anwendung von ϱ^{-1} auf die Indices ξ_1, ξ_2, ξ_3.**

§. 81.

Die Tripelsysteme der Resolventen.

Wir bezeichnen jetzt die Resolvente $\Psi_{\xi_1, \xi_2, \xi_3}$ kürzer durch Ψ^{ξ} und bemerken, dass nach der Formel (2), §. 80 ausser den Quadraten dieser Functionen auch noch gewisse Producte die Permutationen der Gruppe Q gestatten. Zu diesen gehört zunächst das Product aller Grössen Ψ, das wir mit A bezeichnen wollen:

$$A = \prod^{\xi} \Psi_{\xi}, \tag{1}$$

sodann aber die Producte von dreien $\Psi_{\xi}\, \Psi_{\eta}\, \Psi_{\zeta}$, und folglich auch ihre reciproken Werthe

$$v = \frac{1}{\Psi_{\xi}\, \Psi_{\eta}\, \Psi_{\zeta}}, \tag{2}$$

wenn die Indices den Bedingungen genügen:

$$\begin{aligned} \xi_1 + \eta_1 + \zeta_1 &\equiv 0 \\ \xi_2 + \eta_2 + \zeta_2 &\equiv 0 \pmod{2}. \\ \xi_3 + \eta_3 + \zeta_3 &\equiv 0 \end{aligned} \tag{3}$$

Ein solches System von drei Functionen Ψ nennen wir ein Tripel. Ebenso wollen wir drei Indexsysteme $(\xi), (\eta), (\zeta)$, die den Bedingungen (3) genügen, ein Tripel nennen.

Es giebt im Ganzen sieben und nicht mehr solcher Tripel; denn unter den drei Systemen $(\xi), (\eta), (\zeta)$ können nicht zwei einander gleich sein, und durch zwei ist das dritte eindeutig bestimmt. Man kann also für $(\xi), (\eta)$ jedes Paar aus den sieben möglichen Systemen (ξ) nehmen, erhält aber dann jedes Tripel sechsmal. Die Gesammtanzahl ist also $7 . 6 : 6 = 7$.

Um die einzelnen Tripelsysteme zu charakterisiren, führen wir drei nach dem Modul 2 zu nehmende Zahlen $\alpha_1, \alpha_2, \alpha_3$ ein, die nicht alle drei verschwinden, und bemerken, dass die Congruenz

$$\alpha_1 \xi_1 + \alpha_2 \xi_2 + \alpha_3 \xi_3 \equiv 0 \pmod{2} \tag{4}$$

für drei und nur für drei Systeme der Unbekannten ξ_1, ξ_2, ξ_3 befriedigt werden, und dass diese drei ein Tripel bilden, so dass das Tripel durch die drei Congruenzen

$$(5) \qquad \Sigma\, \alpha \xi \equiv 0, \quad \Sigma\, \alpha \eta \equiv 0, \quad \Sigma\, \alpha \zeta \equiv 0 \pmod 2$$

bestimmt ist. Man erkennt dies ohne weitläufige allgemeine Betrachtungen, wenn man die Fälle, in denen nur ein α oder zwei oder alle drei $\alpha \equiv 1 \pmod 2$ sind, einzeln betrachtet.

Da es sieben verschiedene Zahlensysteme $\alpha_1, \alpha_2, \alpha_3$ giebt, so ist durch die Relationen (5) aus jedem solchen Systeme der α ein Tripel völlig bestimmt, und wir können die Function v eindeutig durch $v_{\alpha_1, \alpha_2, \alpha_3}$ oder kürzer durch v_α bezeichnen:

$$(6) \qquad v_\alpha = \frac{1}{\psi_\xi\, \psi_\eta\, \psi_\zeta}.$$

3. Die Functionen v_α, als Functionen der X aufgefasst, gestatten die Permutationen der Gruppe Q.

Wenn wir auf die z eine Substitution σ aus S anwenden, so erleiden nach 2. (§. 80) die ξ, η, ζ gleichzeitig die Substitution ϱ^{-1}; daraus aber ergiebt sich nach (5), dass die α die Substitution σ erleiden, und wir haben also:

4. Die Anwendung der Substitution σ aus S auf die Indices z von X hat die Anwendung derselben Substitution auf die Indices α von v_α zur Folge.

Setzen wir in den Summen (5), in denen $(\xi), (\eta), (\zeta)$ das zu (α) gehörige Tripel ist, für (α) ein anderes System (β), so ist wegen (3)

$$\Sigma \beta \xi + \Sigma \beta \eta + \Sigma \beta \zeta \equiv 0.$$

Ist nun β von α verschieden, so können diese drei Summen nicht alle drei congruent mit 0 sein, weil sonst zwei verschiedene Systeme $(\alpha), (\beta)$ zu demselben Tripel führen würden; folglich müssen von diesen Summen zwei ungerade und eine gerade sein. Wir haben daher den Satz:

5. Durchläuft (ξ) das zu (α) gehörige Tripel, und ist (β) ein von (α) verschiedenes System, so sind unter den Summen $\Sigma \beta \xi$ zwei ungerade und eine gerade.

Wenn wir in der Summe $\Sigma \alpha \xi$ für das System (ξ) alle sieben möglichen Annahmen machen, so erhält man dreimal den Werth 0 und folglich viermal den Werth 1.

Die Congruenz

$$(7) \qquad \Sigma \alpha \xi \equiv 1 \pmod 2$$

hat also vier und nur vier verschiedene Lösungen für ξ. Die Gesammtheit dieser vier Lösungen wollen wir ein **Quadrupel** nennen. Jedes Tripel bestimmt eindeutig ein Quadrupel und umgekehrt, und es giebt also auch sieben verschiedene Quadrupel, die nach (7) durch das Zahlensystem (α) vollständig bestimmt sind. Wir beweisen nun den Satz:

6. Durchläuft (ξ) das zu (α) gehörige Quadrupel und ist (β) ein von (α) verschiedenes System, so sind unter den vier Summen $\Sigma \beta \xi$ zwei gerade und zwei ungerade.

Denn wenn (ξ) die Gesammtheit aller sieben Systeme durchläuft, so finden sich unter den Summen $\Sigma \beta \xi$ drei gerade und vier ungerade; von diesen liefert das zu (α) gehörige Tripel zwei ungerade und eine gerade; es bleiben also für das Quadrupel zwei gerade und zwei ungerade.

Wir ändern nun die Bezeichnung bei den Quadrupeln und nehmen für das System (α) ein anderes Zeichen $(h_1, h_2, h_3) = (h)$. Das zu (h) gehörige Quadrupel bezeichnen wir mit $(\alpha), (\beta), (\gamma), (\delta)$, so dass die vier Congruenzen:

$$(8) \qquad \Sigma h \alpha \equiv 1, \ \Sigma h \beta \equiv 1, \ \Sigma h \gamma \equiv 1, \ \Sigma h \delta \equiv 1 \pmod 2$$

bestehen.

Im Nenner des Productes der vier Functionen

$$v_\alpha, \ v_\beta, \ v_\gamma, \ v_\delta$$

kommen nach (6) im Ganzen 12 Factoren Ψ_ξ vor, und zwar kommt jeder Factor Ψ_ξ so oft darunter vor, als die Anzahl der geraden Zahlen unter den Summen

$$\Sigma \xi \alpha, \ \Sigma \xi \beta, \ \Sigma \xi \gamma, \ \Sigma \xi \delta$$

beträgt, d. h. Ψ_h kommt gar nicht vor, während jedes andere Ψ_ξ zweimal vorkommt (nach 6.).

Wenn wir also noch die Relation (1) benutzen, so ergiebt sich:

$$(9) \qquad \Psi_h^2 = A^2 \, v_\alpha \, v_\beta \, v_\gamma \, v_\delta.$$

Wir stellen für die Anwendung die sieben Tripel zusammen, aus denen man die Quadrupel als die Ergänzung zu dem vollen Systeme ablesen kann. In der ersten Columne steht das Zeichen (α), zu dem das Tripel gehört:

1 0 0	0 1 0	0 0 1	0 1 1
0 1 0	1 0 0	0 0 1	1 0 1
0 0 1	1 0 0	0 1 0	1 1 0
0 1 1	1 0 0	0 1 1	1 1 1
1 0 1	0 1 0	1 0 1	1 1 1
1 1 0	0 0 1	1 1 0	1 1 1
1 1 1	0 1 1	1 0 1	1 1 0

Bezeichnen wir die Symbole (α) in der Reihenfolge, in der sie in der ersten Columne dieser Tabelle stehen, mit 1, 2, 3, 4, 5, 6, 7, so können wir die Tabelle für die Tripel und Quadrupel einfacher so darstellen:

1	2	3	4	1	5	6	7
2	1	3	5	2	4	6	7
3	1	2	6	3	4	5	7
4	1	4	7	2	3	5	6
5	2	5	7	1	3	4	6
6	3	6	7	1	2	4	5
7	4	5	6	1	2	3	7

§. 82.

Anwendung auf Gleichungen 8ten Grades.

In den abgeleiteten Formeln setzen wir nun für die Variablen X_{z_1, z_2, z_3} die Wurzeln einer Gleichung 8ten Grades, von der wir annehmen, dass ihre Galois'sche Gruppe $P = TQ$ in dem festgesetzten Rationalitätsbereiche Ω in der linearen Congruenzgruppe $R = SQ$ enthalten sei, so dass T ein Theiler von S ist. Alle Functionen, die die Permutationen dieser Gruppe gestatten, sind rational.

Dazu gehört zunächst die Summe der X:

(1) $$\sum^{z} X_{z_1, z_2, z_3} = B,$$

ferner die durch (1) des vorigen Paragraphen definirte Grösse A; sodann aber auch die symmetrischen Functionen der sieben Grössen Ψ^2, und ferner, wenn wir nun der Einfachheit halber die Annahme hinzufügen, auf die wir noch zurückkommen, dass von den Grössen Ψ keine verschwinde, die symmetrischen Functionen der Grössen v; aber nicht nur die symmetrischen Functionen der v, sondern alle Functionen der v, die die Permutationen der Gruppe T gestatten.

Die sieben Grössen

$$(2) \qquad \begin{gathered} v_{1,0,0} = v_1, \quad v_{0,1,0} = v_2, \quad v_{0,0,1} = v_3, \\ v_{0,1,1} = v_4, \quad v_{1,0,1} = v_5, \quad v_{1,1,0} = v_6, \quad v_{1,1,1} = v_7 \end{gathered}$$

sind alsdann die Wurzeln einer rationalen Gleichung 7ten Grades mit der Gruppe T, und durch Addition der Gleichung (1) und der Gleichungen [§. 80, (1)]:

$$\Sigma\, (-1)^{\Sigma s \xi} X_{s_1, s_2, s_3} = \Psi_{\xi_1, \xi_2, \xi_3}$$

ergiebt sich mit Rücksicht auf (9) des vorigen Paragraphen:

$$(3) \quad \begin{aligned} 8\, X_{0,0,0} = A \{ & \sqrt{v_1}\sqrt{v_5}\sqrt{v_6}\sqrt{v_7} + \sqrt{v_2}\sqrt{v_4}\sqrt{v_6}\sqrt{v_7} \\ & + \sqrt{v_3}\sqrt{v_4}\sqrt{v_5}\sqrt{v_7} + \sqrt{v_2}\sqrt{v_3}\sqrt{v_5}\sqrt{v_6} \\ & + \sqrt{v_1}\sqrt{v_3}\sqrt{v_4}\sqrt{v_6} + \sqrt{v_1}\sqrt{v_2}\sqrt{v_4}\sqrt{v_5} \\ & + \sqrt{v_1}\sqrt{v_2}\sqrt{v_3}\sqrt{v_7} \} + B. \end{aligned}$$

Es giebt 15 Vorzeichenänderungen der sieben Quadratwurzeln $\sqrt{v}$, bei denen dieser Ausdruck ungeändert bleibt, nämlich, wenn alle sieben Vorzeichen gleichzeitig geändert werden oder wenn die Vorzeichen eines Tripels oder eines Quadrupels geändert werden. Folglich erhält der Ausdruck (3) nur acht verschiedene Werthe, wie man auch die sieben darin vorkommenden Quadratwurzeln bestimmen mag.

§. 83.

Metacyklische Gleichungen 8ten Grades.

Um nun nach diesen Vorbereitungen die primitiven metacyklischen Gleichungen 8ten Grades zu finden, haben wir zunächst die metacyklischen Theiler der Gruppe S zu ermitteln. Die Gruppe S selbst ist, wie schon erwähnt, nicht metacyklisch. Ihre

Theiler haben wir schon betrachtet (§. 70 bis 72), und alle echten Theiler von S sind metacyklisch. Darunter sind Theiler vom 21sten und 7ten Grade, die wir mit T_{21}, T_7 bezeichnen wollen, ferner Theiler vom 24sten Grade, und noch andere Theiler, deren Gradzahlen in 24 aufgehen, die wir hier alle in dem Zeichen T_{24} zusammenfassen wollen.

Diese Gruppen T_{24} können nicht die sieben Grössen $(\xi) = (\xi_1, \xi_2, \xi_3)$ transitiv mit einander verbinden, weil der Grad einer transitiven Permutationsgruppe von sieben Elementen durch 7 theilbar sein muss (Bd. I, §. 154, 7.). Wir wollen nachweisen, dass die den Gruppen $T_{24}\,Q$ entsprechenden Permutationsgruppen der X imprimitiv sind, und dass diese Gruppen daher von unserer Betrachtung ausscheiden[1]).

Da alle Permutationen σ, die zwei der sieben Elemente (ξ) ungeändert lassen oder nur unter einander permutiren, ein drittes Element, nämlich die Ergänzung zum Tripel, ungeändert lassen, so sind zwei Fälle möglich:

1) die Gruppe T_{24} lässt ein Element in Ruhe, oder
2) die sieben Elemente werden in zwei Theile von drei und vier Elementen zerlegt, von denen jeder Theil nur unter sich permutirt wird.

Im letzten Falle können wir die drei Elemente als einem Tripel, und demnach die vier Elemente als einem Quadrupel angehörig betrachten. Denn werden drei Elemente, die nicht einem Tripel angehören, unter sich permutirt, so werden auch die drei Ergänzungen je zweier Elemente zum Tripel unter sich permutirt, und das eine übrig bleibende Element bleibt ungeändert. Wir kommen also auf den Fall 1) zurück.

Wir fügen nun zu den sieben Systemen (ξ) noch das achte $(0, 0, 0) = (0)$ hinzu und bezeichnen die acht Grössen X_{ξ_1, ξ_2, ξ_3} mit

(1) $$0, 1, 2, 3, 4, 5, 6, 7.$$

Im Falle 1) bleiben dann durch die Substitutionen von T_{24} zwei dieser acht Elemente, etwa 0, 1, ungeändert. Es giebt ferner in Q eine und nur eine Substitution γ_0, durch die 0 mit 1 vertauscht wird.

---

[1]) Aus der Literatur über die Gleichungen 8ten Grades ist zu erwähnen: Nöther, Mathem. Annalen, Bd. XV. Wilshaus, Ueber die algebraische Auflösbarkeit der Gleichungen 8ten Grades. Dissertation. Marburg 1888.

Die beiden Substitutionen $1, \gamma_0$ bilden eine Gruppe Q_0. Irgend eine Substitution γ_1 von Q, die nicht in Q_0 vorkommt, führt 0, 1 in zwei davon verschiedene Elemente, etwa 2, 3, über, und durch die zwei Substitutionen $Q_0 \gamma_1$ geht 0, 1 in 2, 3 oder in 3, 2 über. Wenn ferner durch γ_2 das Paar 0, 1 in ein drittes Paar 4, 5 übergeht, so ist 4, 5 sowohl von 0, 1 als von 2, 3 verschieden, und so können wir Q in die Nebengruppen zerlegen:

$$Q = Q_0 + Q_0 \gamma_1 + Q_0 \gamma_2 + Q_0 \gamma_3,$$

wodurch die acht Elemente (1) in vier Paare

(2) $$0, 1; \quad 2, 3; \quad 4, 5; \quad 6, 7$$

zerlegt sind, so dass durch die beiden Substitutionen einer der Nebengruppen $Q_0 \gamma_i$ das Paar 0, 1 in eines dieser vier Paare übergeht.

Ist nun k irgend eine Substitution aus der Gruppe

$$P = T_{24} Q,$$

so lassen sich die Elemente $\tau_0, \tau_1, \tau_2, \tau_3$ aus T_{24} und $\gamma_0', \gamma_1', \gamma_2', \gamma_3'$ aus Q so bestimmen, dass

$$k = \tau_0 \gamma_0', \quad \gamma_1 k = \tau_1 \gamma_1', \quad \gamma_2 k = \tau_2 \gamma_2', \quad \gamma_3 k = \tau_3 \gamma_3'$$

oder

$$k = \tau_0 \gamma_0' = \gamma_1^{-1} \tau_1 \gamma_1' = \gamma_2^{-1} \tau_2 \gamma_2' = \gamma_3^{-1} \tau_3 \gamma_3',$$

und diese Darstellung zeigt, dass durch k irgend eines der Paare (2) in ein Paar desselben Systems übergeführt wird; denn z. B. durch γ_1^{-1} wird 2, 3 in 0, 1 übergeführt, durch τ_1 bleibt 0, 1 ungeändert und durch γ_1', was zu Q gehört, wird 0, 1 in eines der Paare (2) übergeführt.

Die Gruppe $T_{24} Q$ ist also imprimitiv, und zwar so, dass wir vier Systeme der Imprimitivität haben. Die Wurzeln 0, 1 genügen einer quadratischen Gleichung, deren Coëfficienten von den Wurzeln einer biquadratischen Gleichung abhängen.

Gehen wir nun zu dem Falle 2) über, in dem die Elemente je eines Tripels 1, 2, 3 und eines Quadrupels 4, 5, 6, 7 durch T_{24} transitiv unter einander verbunden sind. Die acht Grössen (1) zerfallen hier in zwei Quadrupel:

(3) $$0, 1, 2, 3; \quad 4, 5, 6, 7,$$

und durch die Substitutionen von Q werden die Grössen eines dieser Quadrupel entweder nur unter sich vertauscht, oder sie werden in die Grössen des anderen Quadrupels übergeführt.

Um dies einzusehen, bezeichnen wir in der früheren Bezeichnungsweise 1, 2, 3 mit (ξ), (η), (ζ); da diese drei Grössen ein Tripel bilden, so giebt es [nach §. 81, (5)] ein System (α), so dass

(4) $$\Sigma \alpha \xi \equiv 0, \ \Sigma \alpha \eta \equiv 0, \ \Sigma \alpha \zeta \equiv 0 \pmod 2$$

ist. Wenden wir nun eine Substitution aus Q an:

$$\begin{pmatrix} \xi_1, & \xi_2, & \xi_3 \\ \xi_1', & \xi_2', & \xi_3' \end{pmatrix},$$

worin $\xi_i' = \xi_i + h_i$ sein mag, so folgt aus (4):

$$\Sigma \alpha \xi' \equiv \Sigma \alpha \eta' \equiv \Sigma \alpha \zeta' \equiv \Sigma \alpha h,$$

d. h. die (ξ'), (η'), (ζ') bilden das zu (α) gehörige Tripel, wenn (h) selbst zu diesem Tripel gehört, oder im anderen Falle ist (h), (ξ'), (η'), (ζ'), das zu (α) gehörige Quadrupel.

Bezeichnet also nun wieder k irgend eine Substitution aus P und γ eine Substitution aus Q, durch die das Quadrupel 0, 1, 2, 3 in 4, 5, 6, 7 übergeht, so können wir die Elemente τ', τ'' aus T_{24} und γ', γ'' aus Q so bestimmen, dass

$$k = \tau' \gamma' = \gamma^{-1} \tau'' \gamma'',$$

wodurch, wie oben, bewiesen wird, dass die beiden Systeme (3) durch k imprimitiv verbunden sind.

Nach Adjunction einer Quadratwurzel zum Rationalitätsbereiche sind dann die Grössen 0, 1, 2, 3 die Wurzeln einer biquadratischen Gleichung.

Durch diese Betrachtungen wird für primitive Gleichungen 8ten Grades auch die Möglichkeit ausgeschlossen, dass eine der sieben Grössen $\Psi_{\xi_1, \xi_2, \xi_3}$ [§. 80, (1)] verschwinde. Diese Functionen sind nämlich rationale Functionen der Wurzeln X; wenn also eine von ihnen verschwindet, so kann auf die rationale Gleichung $\Psi = 0$ jede Permutation der Gruppe der Gleichung angewandt werden. Daraus ergiebt sich nach dem Theorem §. 80, 2., dass entweder alle sieben Functionen Ψ verschwinden müssen, in welchem Falle die Wurzeln rational wären, oder dass die Substitutionen ϱ^{-1}, auf die (ξ) angewandt, eine intransitive Gruppe bilden müssen. Der Grad der Gruppe könnte dann nicht durch 7 theilbar sein. Nun ist die Gruppe der ϱ^{-1} isomorph mit der Gruppe T der σ (§. 37, 8.), und daher ist auch der Grad von T nicht durch 7 theilbar, und folglich ist

auch T intransitiv. Daraus folgt, wie oben gezeigt, dass TQ imprimitiv ist.

Als Gruppe für primitive metacyklische Gleichungen 8ten Grades bleiben also nur die beiden Typen

$$T_7 Q, \quad T_{21} Q$$

übrig. Im ersten Falle sind die in der Formel [§. 82, (3)] vorkommenden Grössen v die Wurzeln einer cyklischen Gleichung 7ten Grades mit der Gruppe $(z, z+b)$, im zweiten einer metacyklischen mit der Gruppe $(z, az+b)$ (Bd. I, §. 180), worin z, a, b nach dem Modul 7 genommen sind und a die Werthe 1, 2, 4 durchläuft.

Um eine Zuordnung der v_i, wie sie in der Formel (3), §. 82 vorkommen, zu den v_z, worin z der in den Gruppen $(z, z+b)$ oder $(z, az+b)$ vorkommende Index ist, zu erhalten, können wir von einer beliebigen Substitution siebenter Ordnung ausgehen, etwa von

$$\tau = \begin{pmatrix} 1, & 0, & 1 \\ 1, & 0, & 0 \\ 0, & 1, & 0 \end{pmatrix} \quad [\S.\ 79,\ (2)].$$

Nehmen wir dann $v_{1,0,0}$ für v_0, so findet man durch wiederholte Anwendung von τ auf 1, 0, 0 folgende Anordnung:

$$(1,0,0)=0,\ (1,1,0)=1,\ (1,1,1)=2,\ (0,1,1)=3,\ (1,0,1)=4,$$
$$(0,1,0)=5,\ (0,0,1)=6,$$

und nach §. 82, (2) hat man daher

$$v_1,\ v_2,\ v_3,\ v_4,\ v_5,\ v_6,\ v_7$$

durch

$$v_0,\ v_5,\ v_6,\ v_3,\ v_4,\ v_1,\ v_2$$

zu ersetzen. Dadurch ergiebt sich aus §. 82, (3):

$$8X = A \sum_{0,6}^{z} \sqrt{v_z}\,\sqrt{v_{z+1}}\,\sqrt{v_{z+2}}\,\sqrt{v_{z+4}} + B,$$

worin A, B rationale Grössen, und v_z die Wurzeln einer cyklischen oder einer metacyklischen Gleichung von der Gruppe $(z, az+b)$ vom Grade 7 sind.

Umgekehrt ist es auch nicht schwer, nachzuweisen, dass die acht durch Wechsel der Vorzeichen hieraus abgeleiteten Grössen immer die Wurzeln einer primitiven metacyklischen Gleichung

8ten Grades sind, worauf hier nicht näher eingegangen werden soll (vgl. Bd. I, §. 185).

§. 84.

Biquadratische Gleichungen.

Wir haben uns auf die Betrachtung der primitiven metacyklischen Gleichungen 8ten Grades beschränkt, weil die imprimitiven auf Gleichungen 4ten Grades zurückkommen. Um also auch die Wurzeln der letzteren in der Weise des vorigen Paragraphen darstellen zu können, haben wir noch eine analoge Darstellung der Wurzeln biquadratischer Gleichungen zu suchen. Hierbei sind dieselben Betrachtungen, wie im §. 82, nur in wesentlich einfacherer Gestalt anwendbar.

Wir bezeichnen die Wurzeln der biquadratischen Gleichung mit

(1) $$X_{0,0},\ X_{1,0},\ X_{0,1},\ X_{1,1},$$

und können dann die ganze Permutationsgruppe 24sten Grades als binäre lineare Congruenzgruppe für den Modul 2 darstellen:

(2) $$P = S\,Q.$$

Die darin enthaltene homogene Gruppe S ist vom 6ten Grade und besteht aus den Substitutionen

(3) $$\sigma = \begin{pmatrix}1, 0\\ 0, 1\end{pmatrix},\ \begin{pmatrix}1, 0\\ 1, 1\end{pmatrix},\ \begin{pmatrix}0, 1\\ 1, 0\end{pmatrix},\ \begin{pmatrix}0, 1\\ 1, 1\end{pmatrix},\ \begin{pmatrix}1, 1\\ 1, 0\end{pmatrix},\ \begin{pmatrix}1, 1\\ 0, 1\end{pmatrix},$$

und man kann

(4) $$\sigma_1 = \begin{pmatrix}0, 1\\ 1, 0\end{pmatrix},\quad \sigma_2 = \begin{pmatrix}1, 1\\ 0, 1\end{pmatrix}$$

als die erzeugenden Substitutionen der Gruppe S ansehen.

Wir definiren nun wie im §. 80 die drei Grössen:

(5) $$\begin{aligned} \Psi_{1,0} &= X_{0,0} - X_{1,0} + X_{0,1} - X_{1,1} \\ \Psi_{0,1} &= X_{0,0} + X_{1,0} - X_{0,1} - X_{1,1} \\ \Psi_{1,1} &= X_{0,0} - X_{1,0} - X_{0,1} + X_{1,1}, \end{aligned}$$

so dass $\Psi^2_{1,0}$, $\Psi^2_{0,1}$, $\Psi^2_{1,1}$, aber auch das Product $\Psi_{1,0}\,\Psi_{0,1}\,\Psi_{1,1}$ durch die Substitutionen der cyklischen Gruppe Q ungeändert bleiben

Wendet man auf die Indices ξ, η der X die Substitution σ an, so erleiden die Indices der Ψ [wie im §. 80, (2)] die Substitution ϱ^{-1}, wenn ϱ die transponirte Substitution von σ ist.

Es ist aber, den Substitutionen (4) entsprechend,

$$(6) \qquad \varrho_1^{-1} = \begin{pmatrix} 0, & 1 \\ 1, & 0 \end{pmatrix}, \quad \varrho_2^{-1} = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}.$$

Indem wir nun der Einfachheit halber voraussetzen, dass die drei Grössen (5) von Null verschieden sind, setzen wir

$$(7) \qquad \begin{aligned} v_{1,0} &= \frac{\Psi_{0,1}\,\Psi_{1,1}}{\Psi_{1,0}} = \frac{\Psi_{0,1}\,\Psi_{1,0}\,\Psi_{1,1}}{\Psi_{1,0}^2}; \\ v_{0,1} &= \frac{\Psi_{1,0}\,\Psi_{1,1}}{\Psi_{0,1}} = \frac{\Psi_{0,1}\,\Psi_{1,0}\,\Psi_{1,1}}{\Psi_{0,1}^2}; \\ v_{1,1} &= \frac{\Psi_{1,0}\,\Psi_{0,1}}{\Psi_{1,1}} = \frac{\Psi_{1,0}\,\Psi_{0,1}\,\Psi_{1,1}}{\Psi_{1,1}^2}. \end{aligned}$$

Die Grössen $v_{\xi,\eta}$ bleiben durch die Substitutionen von Q ungeändert und erleiden durch σ_1, σ_2 die durch (6) bestimmten Permutationen

$$\begin{array}{ll} & v_{1,0},\ v_{0,1},\ v_{1,1} \\ \sigma_1 & v_{0,1},\ v_{1,0},\ v_{1,1} \\ \sigma_2 & v_{1,1},\ v_{0,1},\ v_{1,0}. \end{array}$$

Daraus ergiebt sich, dass die symmetrischen Functionen der drei Grössen $v_{1,0}, v_{0,1}, v_{1,1}$ durch die Permutationen P ungeändert bleiben, und folglich in dem Rationalitätsbereiche der symmetrischen Functionen der X enthalten sind. Die drei Grössen v sind also die Wurzeln einer cubischen Gleichung, und es würde keine Schwierigkeit haben, diese cubische Resolvente der allgemeinen biquadratischen Gleichung zu bilden.

Aus (7) folgt aber ferner

$$v_{1,0}\, v_{0,1} = \psi_{1,1}^2, \quad v_{1,0}\, v_{1,1} = \psi_{0,1}^2, \quad v_{0,1}\, v_{1,1} = \psi_{1,0}^2,$$

und demnach ergiebt sich aus (5), wenn wir noch die rationale Grösse

$$X_{0,0} + X_{1,0} + X_{0,1} + X_{1,1} = a$$

setzen,

$$(8) \qquad 4\, X_{0,0} = a + \sqrt{v_{1,0}}\,\sqrt{v_{0,1}} + \sqrt{v_{1,0}}\,\sqrt{v_{1,1}} + \sqrt{v_{0,1}}\,\sqrt{v_{1,1}}.$$

Der Ausdruck (8) giebt nur vier verschiedene Werthe, wenn wir die Vorzeichen der drei darin vorkommenden Quadratwurzeln auf alle mögliche Arten bestimmen, und man kann auch um-

gekehrt leicht zeigen, dass die vier in der Form (8) enthaltenen Grössen X, wenn die $v_{1,0}$, $v_{0,1}$, $v_{1,1}$ die Wurzeln irgend einer cubischen Gleichung sind, einer biquadratischen Gleichung mit rationalen Coëfficienten genügen [1]).

---

1) Diese Form der Lösung der biquadratischen Gleichung ist das Analogon zu der Cayley'schen Form der Cardanischen Formel (Bd. I, §. 36). Ich weiss nicht, ob diese Form der Auflösung biquadratischer Gleichungen in der elementaren Algebra sonst schon bekannt ist. Ich habe sie zuerst in einer englischen Aufgaben-Sammlung „Mathematical Tripos, Part I, June 1894" gefunden, wo auch die cubische Resolvente der v gebildet ist.

Elfter Abschnitt.

Die Wendepunkte einer Curve dritter Ordnung.

---

§. 85.

Ternäre Formen und algebraische Curven.

Um im weiteren Verlauf unserer Darstellung dem Leser einige von den mannigfaltigen und interessanten Anwendungen der Algebra auf geometrische Probleme vorführen zu können, ohne ihn auf andere Hülfsmittel zu verweisen, sollen hier die nothwendigen geometrischen Grundlagen für diese Anwendungen in der Kürze abgeleitet werden. Wir beschränken uns dabei auf die Geometrie der Ebene und lassen auch da Alles bei Seite, was für unsere Anwendungen nicht direct erforderlich ist [1].

Wir wenden die homogenen Dreieckscoordinaten an, die dadurch erklärt sind, dass die Lage eines Punktes x durch seine Abstände von den drei Seiten des Coordinatendreiecks, in drei beliebigen Maasseinheiten gemessen (oder mit drei beliebigen constanten Factoren multiplicirt), bestimmt sind. Diese drei Grössen heissen die Coordinaten des Punktes x, und werden meist mit x_1, x_2, x_3 oder mit y_1, y_2, y_3 etc. bezeichnet.

Zwischen diesen drei Coordinaten des Punktes x besteht eine lineare, nicht homogene Relation, die man erhält, wenn man den Flächeninhalt des Coordinatendreiecks (1, 2, 3) gleich der Summe der Inhalte der drei Dreiecke (x, 2, 3), (x, 3, 1), (x, 1, 2) setzt. Eine Coordinate und also auch der Ausdruck für den Flächeninhalt des entsprechenden der drei letztgenannten Drei-

---

[1]) Ausführlicheres findet man in den Lehrbüchern der analytischen Geometrie, unter denen das Werk von George Salmon, „Higher plane curves“, deutsch von Fiedler, hervorzuheben ist.

ecke ändern ihr Vorzeichen, so oft der Punkt x durch eine Seite des Coordinatendreiecks hindurchgeht.

Mit Hülfe dieser nicht homogenen Relation kann die Einheit linear und homogen durch x_1, x_2, x_3 dargestellt und dadurch jede nicht homogene Function in eine homogene verwandelt werden.

Die Coordinaten x_1, x_2, x_3 sind nach diesen Bestimmungen zunächst nicht unabhängige Variable, sondern an die erwähnte Relation gebunden. Wir erweitern ihre Bedeutung aber jetzt so, dass wir sie als unabhängige Variable betrachten können, wenn wir festsetzen, dass wir sie nur in homogenen Formen oder Gleichungen benutzen wollen, und dass nicht x_1, x_2, x_3 selbst, sondern nur die Verhältnisse $x_1 : x_2 : x_3$ die Lage des Punktes x bestimmen sollen. Dann können wir von der erwähnten Relation zwischen den x_1, x_2, x_3 ganz absehen, und die x_1, x_2, x_3 als unabhängige Variable betrachten, für die nur die einzige Werthcombination $x_1 = 0$, $x_2 = 0$, $x_3 = 0$ ausgeschlossen ist. Die Werthe $h x_1, h x_2, h x_3$ bestimmen dann für jedes von Null verschiedene h einen und denselben Punkt x. Genau gesagt, sind dann die Coordinaten x_1, x_2, x_3 des Punktes x nicht die oben beschriebenen Abstände von den Coordinatenaxen selbst, sondern irgend welche Grössen, die mit diesen Abständen proportional sind.

Jede lineare Substitution

$$(1)\qquad \begin{aligned} x_1 &= \alpha_1^{(1)} y_1 + \alpha_1^{(2)} y_2 + \alpha_1^{(3)} y_3 \\ x_2 &= \alpha_2^{(1)} y_1 + \alpha_2^{(2)} y_2 + \alpha_2^{(3)} y_3 \\ x_3 &= \alpha_3^{(1)} y_1 + \alpha_3^{(2)} y_2 + \alpha_3^{(3)} y_3, \end{aligned}$$

deren Determinante

$$(2)\qquad r = \Sigma \pm \alpha_1^{(1)} \alpha_2^{(2)} \alpha_3^{(3)}$$

von Null verschieden ist, kann in doppelter Weise geometrisch gedeutet werden, einmal als eine Abbildung, indem wir x_1, x_2, x_3 und y_1, y_2, y_3 als Coordinaten zweier Punkte x, y in demselben Coordinatensysteme ansehen, so dass jedem Punkte y ein Punkt x entspricht und umgekehrt, sodann auch als Coordinatentransformation, wenn wir x_1, x_2, x_3 und y_1, y_2, y_3 als Coordinaten eines und desselben Punktes, bezogen auf zwei verschiedene Coordinatensysteme, betrachten. Für die nächsten Betrachtungen werden wir an der letzteren Interpretation festhalten.

Irgend eine ternäre Form n^{ten} Grades $f(x_1, x_2, x_3)$ stellt, gleich Null gesetzt, eine Curve n^{ter} Ordnung dar, die mit einer geraden Linie n Schnittpunkte hat. Diese Curve bezeichnen wir kurz als die Curve f.

Durch die Substitution (1) geht f in eine andere Form desselben Grades in den Variablen y_1, y_2, y_3 über:

(3) $$f(x_1, x_2, x_3) = \varphi(y_1, y_2, y_3),$$

und $\varphi = 0$ stellt dieselbe Curve dar, wie $f = 0$, bezogen auf das Coordinatensystem y_1, y_2, y_3.

Bilden wir die Ableitungen der Identität (3) nach den Variablen y_1, y_2, y_3, so folgt mit Rücksicht auf (1):

(4) $$\begin{aligned} \varphi'(y_1) &= \alpha_1^{(1)} f'(x_1) + \alpha_2^{(1)} f'(x_2) + \alpha_3^{(1)} f'(x_3) \\ \varphi'(y_2) &= \alpha_1^{(2)} f'(x_1) + \alpha_2^{(2)} f'(x_2) + \alpha_3^{(2)} f'(x_3) \\ \varphi'(y_3) &= \alpha_1^{(3)} f'(x_1) + \alpha_2^{(3)} f'(x_2) + \alpha_3^{(3)} f'(x_3). \end{aligned}$$

§. 86.

Singuläre Punkte. Wendepunkte. Doppeltangenten.

Wenn für einen Punkt x die drei Gleichungen

(1) $$f'(x_1) = 0, \quad f'(x_2) = 0, \quad f'(x_3) = 0$$

zugleich erfüllt sind, so liegt nach dem Euler'schen Theorem

(2) $$nf = x_1 f'(x_1) + x_2 f'(x_2) + x_3 f'(x_3)$$

(Bd. I, §. 17) dieser Punkt auf der Curve f. Die Gleichungen §. 85, (4) zeigen, dass in demselben Punkte auch $\varphi'(y_1)$, $\varphi'(y_2)$, $\varphi'(y_3)$ verschwinden müssen, dass also die durch die Gleichungen (1) charakterisirte Eigenschaft eines Punktes bei linearer Transformation erhalten bleibt, also, wie wir uns auch ausdrücken, zu den invarianten Eigenschaften gehört.

Nicht auf jeder Curve n^{ter} Ordnung kommen Punkte vor, die den Bedingungen (1) genügen, wie z. B. die Annahme $f(x_1, x_2, x_3) = x_1^n + x_2^n + x_3^n$ zeigt. Es wird vielmehr, wenn auch nur ein solcher Punkt existiren soll, eine Gleichung zwischen den Coëfficienten von f erfüllt sein müssen, die man durch Elimination von x_1, x_2, x_3 aus den drei Gleichungen (1) erhält (Bd. I, §. 50). Man kann diese Relation in der Form darstellen, dass eine gewisse ganze rationale und homogene Function der sämmtlichen Coëfficienten von f gleich Null sein muss, und diese Function

heisst die Discriminante von f. Sie ist durch diese Definition nur bis auf einen numerischen Factor bestimmt, und kann bis jetzt nur in den einfachsten Fällen berechnet werden.

Die Punkte der Curve f, deren Coordinaten den Bedingungen (1) genügen, heissen singuläre Punkte.

Man kann auch die Frage aufwerfen, unter welcher Bedingung es möglich ist, dass auf einer Curve unendlich viele singuläre Punkte vorkommen. Damit dies eintritt, muss zunächst das Eliminationsresultat von einer der Unbekannten, etwa von x_3, aus den zwei Gleichungen $f'(x_1) = 0$, $f'(x_2) = 0$ identisch verschwinden, d. h. die beiden Functionen $f'(x_1)$ und $f'(x_2)$ müssen, als Functionen von x_3 betrachtet, einen gemeinschaftlichen Theiler haben, und nach Bd. I, §. 51 müssen sie daher auch einen (nicht constanten) gemeinsamen Theiler im Gebiete der Formen x_1, x_2, x_3 haben. Dieser Theiler muss dann wieder, wie aus denselben Erwägungen hervorgeht, einen gemeinschaftlichen Theiler mit f, oder, was dasselbe ist, mit $f'(x_3)$ haben, und es ergiebt sich also, dass nur dann unendlich viele singuläre Punkte vorhanden sein können, wenn die vier Formen $f, f'(x_1), f'(x_2), f'(x_3)$ einen gemeinschaftlichen Theiler haben.

Es sei nun u ein solcher gemeinschaftlicher Theiler, den wir als irreducibel voraussetzen.

Wir setzen

$$f(x_1, x_2, x_3) = uv$$

$$f'(x_1) = u\frac{\partial v}{\partial x_1} + v\frac{\partial u}{\partial x_1}$$

$$f'(x_2) = u\frac{\partial v}{\partial x_2} + v\frac{\partial u}{\partial x_2}$$

$$f'(x_3) = u\frac{\partial v}{\partial x_3} + v\frac{\partial u}{\partial x_3},$$

und diese Gleichungen zeigen, da u irreducibel ist und daher

$$u, \frac{\partial u}{\partial x_1}, \frac{\partial u}{\partial x_2}, \frac{\partial u}{\partial x_3}$$

keinen gemeinschaftlichen Theiler haben können, dass v durch u theilbar sein muss; d. h. es können nur dann unendlich viele singuläre Punkte vorkommen, wenn $f(x_1, x_2, x_3)$ einen quadratischen Theiler hat. In diesem Falle sagen wir, dass die Curve f einen doppelt zählenden Bestandtheil enthält.

Um die geometrische Bedeutung der singulären Punkte zu erkennen, denken wir uns die Function f nach Potenzen der einen Variablen x_3 geordnet:

(2) $$f(x_1, x_2, x_3) = x_3^n f_0 + x_3^{n-1} f_1 + x_3^{n-2} f_2 + \cdots,$$

worin $f_0, f_1, f_2, \ldots$ binäre Formen der Variablen x_1, x_2 sind, deren Grad durch den Index angegeben ist, so dass f_0 eine Constante, f_1 eine lineare, f_2 eine quadratische Form ist u. s. f.

Wenn nun ein singulärer Punkt vorhanden ist, so können wir wegen der Invarianz dieser Eigenschaft annehmen, dass dieser Punkt in die Ecke $x_1 = 0$, $x_2 = 0$ des Coordinatendreiecks, die wir mit ξ_3 bezeichnen wollen, falle. Dann müssen f_0 und f_1 verschwinden, und wenn wir dann $x_1 = 0$ setzen, so erhält die Gleichung $f = 0$ den Factor x_2^2. Dies besagt, dass zwei der Schnittpunkte der Linie $x_1 = 0$ in dem singulären Punkte zusammenfallen. Die Linie $x_2 = 0$ kann aber jede durch den singulären Punkt hindurchgehende Gerade sein, und so folgt, dass der singuläre Punkt die Eigenschaft hat, dass jede durch ihn hindurchgehende Gerade die Curve dort in zwei zusammenfallenden Punkten schneidet.

Aus diesem Grunde nennt man die singulären Punkte auch Doppelpunkte; womit aber nicht ausgeschlossen ist, dass auch mehr als zwei Schnittpunkte zusammenfallen können, wodurch die höheren Singularitäten entstehen.

An die Form der Gleichung (2) knüpfen wir noch einige in der Folge wichtige einfache Betrachtungen.

Wenn der Punkt ξ_3 auf der Curve f liegt, aber kein singulärer Punkt ist, so muss die Constante f_0 verschwinden und $f_1 = 0$ ist die Gleichung der Tangente der Curve in diesem Punkte. Nehmen wir diese Tangente für die Linie $x_1 = 0$, so lautet die Gleichung der Curve, wenn wir einen constanten Factor gleich 1 annehmen:

(3) $$f = x_3^{n-1} x_1 + x_3^{n-2} f_2 + \cdots = 0.$$

Wenn die quadratische Form f_2 durch x_1 theilbar ist, so erhält die Gleichung (3) für $x_1 = 0$ den Factor x_2^3 und der Punkt ξ_3 zählt als dreifacher Schnittpunkt von $x_1 = 0$ mit der Curve. Ein solcher Punkt heisst ein Wendepunkt oder Inflexionspunkt der Curve f, und $x_1 = 0$ heisst die Wendetangente. Die Wendepunkte gehören nicht zu den singulären Punkten.

Ist der Punkt ξ_3 ein Wendepunkt und $x_1 = 0$ die Wendetangente, so hat f die Gestalt

$$(4) \qquad f = x_1 \varphi + x_2^3 \psi,$$

worin φ eine Form $(n-1)^{\text{ten}}$, ψ eine Form $(n-3)^{\text{ten}}$ Grades ist.

Umgekehrt ist, wenn f diese Form hat, der Punkt ξ_3 ein Wendepunkt, und $x_1 = 0$ die Wendetangente.

Eine gerade Linie, die die Curve f in zwei getrennten Punkten berührt, heisst eine Doppeltangente. Nehmen wir eine solche Doppeltangente zur Linie $x_3 = 0$ und die Berührungspunkte als die auf $x_3 = 0$ gelegenen Ecken des Coordinatendreiecks, so muss, wenn $x_3 = 0$ in $f = 0$ eingesetzt wird, eine Gleichung entstehen, die sowohl x_1 als x_2 zum quadratischen Factor hat. Die Function f muss also die Gestalt haben:

$$(4) \qquad f = x_3 \varphi + x_1^2 x_2^2 \psi,$$

worin φ eine Form $(n-1)^{\text{ten}}$ Grades, ψ eine Form $(n-4)^{\text{ten}}$ Grades ist.

Etwas allgemeiner können wir auch sagen: Wenn $x_3 = 0$ eine Doppeltangente ist, so kann f so dargestellt werden:

$$(5) \qquad f = x_3 \varphi + \chi^2 \psi,$$

worin $\chi = 0$ die Gleichung eines Kegelschnittes ist. Die Berührungspunkte der Doppeltangente sind die Schnittpunkte von $x_3 = 0$ und $\chi = 0$.

§. 87.

Fundamentale Covarianten einer ternären Form.

Im §. 60 des ersten Bandes haben wir den Begriff der Invarianten und Covarianten einer Form kennen gelernt. Auch in der Geometrie spielen diese Formen eine grosse Rolle.

Wenn durch die lineare Substitution §. 85, (1) die ternäre Form $f(x_1, x_2, x_3)$, die wir abgekürzt auch mit $f(x)$ bezeichnen, in $\varphi(y)$ übergeht, und wenn wir mit a die Coëfficienten von f, mit b die Coëfficienten von φ und mit r die Substitutionsdeterminante bezeichnen, so heisst eine Form $\Phi(x, a)$, die sowohl in Bezug auf die x wie in Bezug auf die a homogen ist, eine Covariante von $f(x)$, wenn sie der Bedingung

$$(1) \qquad \Phi(y, b) = r^{\lambda} \Phi(x, a)$$

genügt. Wenn insbesondere die Form von den Variablen x unabhängig und nur von den Coëfficienten a abhängig ist, so wird sie zur Invariante. Der Exponent λ, der das Gewicht der Covariante heisst, ist eine ganze Zahl.

Wir haben im Bd. I, §. 59 eine bei allen Formen, deren Grad grösser als 1 ist, vorhandene Covariante vom Gewicht 2 kennen gelernt, nämlich die Hesse'sche Determinante:

$$(2)\qquad H(x_1, x_2, x_3) = \begin{vmatrix} f''(x_1, x_1), f''(x_1, x_2), f''(x_1, x_3) \\ f''(x_2, x_1), f''(x_2, x_2), f''(x_2, x_3) \\ f''(x_3, x_1), f''(x_3, x_2), f''(x_3, x_3) \end{vmatrix}.$$

Ausser dieser Covariante H wollen wir noch zwei andere allgemeine Covarianten betrachten, die bei allen ternären Formen von höherem als dem 2ten Grade existiren, und die sich leicht auch für Formen von beliebig vielen Variablen verallgemeinern lassen. Die erste dieser Formen ist, wenn H wie oben die Hesse'sche Covariante bedeutet:

$$(3)\qquad C_1(x, a) = \begin{vmatrix} f''(x_1,x_1), f''(x_1,x_2), f''(x_1,x_3), H'(x_1) \\ f''(x_2,x_1), f''(x_2,x_2), f''(x_2,x_3), H'(x_2) \\ f''(x_3,x_1), f''(x_3,x_2), f''(x_3,x_3), H'(x_3) \\ H'(x_1), \quad H'(x_2), \quad H'(x_3) \quad 0 \end{vmatrix}.$$

Um die Invarianten-Eigenschaft für diese Form nachzuweisen, machen wir darin die Substitution §. 85, (1). Dadurch geht $f(x, a)$ in $\varphi(y, b)$ und $r^2 H(x, a)$ in $H(y, b)$ über. Wenn wir dann unter $H'(y_1)$, $H'(y_2)$, $H'(y_3)$ die Derivirten von $H(y, b)$ verstehen, so haben wir die Formeln

$$(4)\qquad \begin{aligned} \varphi''(y_\mu, y_\nu) &= \sum^{i,k} f''(x_i, x_k)\, \alpha_i^{(\mu)} \alpha_k^{(\nu)} \\ H'(y_\nu) &= r^2 \sum^{i} H'(x_i)\, \alpha_i^{(\nu)}, \end{aligned}$$

in denen μ, ν, i, k von 1 bis 3 laufen.

Multiplicirt man nun die Determinante $C_1(x, a)$ zweimal nach einander mit der in der Form

$$r = \begin{vmatrix} \alpha_1^{(1)}, & \alpha_1^{(2)}, & \alpha_1^{(3)}, & 0 \\ \alpha_2^{(1)}, & \alpha_2^{(2)}, & \alpha_2^{(3)}, & 0 \\ \alpha_3^{(1)}, & \alpha_3^{(2)}, & \alpha_3^{(3)}, & 0 \\ 0, & 0, & 0, & 1 \end{vmatrix}$$

geschriebenen Substitutionsdeterminante, indem man das eine

Mal nach Zeilen, das andere Mal nach Columnen multiplicirt, so folgt nach den Formeln (4):

(5) $$C_1(y, b) = r^6 C_1(x, a),$$

wodurch die Invarianten-Eigenschaft ausgedrückt und das Gewicht $= 6$ bestimmt ist.

Die dritte Covariante C_2, die wir betrachten, ist die Functionaldeterminante aus den drei Formen f, H, C_1, also

(6) $$C_2(x, a) = \begin{vmatrix} f'(x_1), & H'(x_1), & C_1'(x_1) \\ f'(x_2), & H'(x_2), & C_1'(x_2) \\ f'(x_3), & H'(x_3), & C_1'(x_3) \end{vmatrix},$$

die, wie schon aus §. 59 des ersten Bandes hervorgeht, die Invarianten-Eigenschaft hat:

(7) $$C_2(y, b) = r^9 C_2(x, a),$$

und die also das Gewicht 9 hat.

Bezeichnen wir mit λ das Gewicht, mit ν den Grad in den Variablen, mit μ den Grad in den Coëfficienten, so ergiebt sich folgende Zusammenstellung:

	ν,	μ,	λ
f	n,	1,	0
H	$3n - 6$,	3,	2
C_1	$8n - 18$,	8,	6
C_2	$12n - 27$,	12,	9.

§. 88.

Die Hesse'sche Curve.

Die erste der eingeführten Covarianten H hat eine einfache geometrische Bedeutung, die wir jetzt kennen lernen wollen. Diese Untersuchung wird dadurch wesentlich erleichtert, dass wir, wegen der Invarianten-Eigenschaft der Form H, nichts an Allgemeinheit verlieren, wenn wir dem Coordinatensysteme irgend eine specielle Lage gegen die Curve f geben.

Legen wir die Ecke ξ_3 des Coordinatendreiecks in einen Punkt der Curve f, der nicht zu den singulären gehört, und wählen die Tangente in diesem Punkte zur x_1-Axe, so erhält nach §. 86, (3) die Form f den Ausdruck:

(1) $$f = h x_3^{n-1} x_1 + x_3^{n-2}(a x_1^2 + 2 b x_1 x_2 + c x_2^2) + x_3^{n-3} f_3 + \cdots,$$

worin h, a, b, c Constanten sind, von denen h von Null verschieden ist, und f_3 eine binäre cubische Form von x_1, x_2.

Wenn wir hiernach die nach absteigenden Potenzen von x_3 geordnete Function H berechnen:

$$(2) \qquad H = x_3^{3n-6} H_0 + x_3^{3n-7} H_1 + \cdots,$$

so findet sich

$$(3) \qquad \begin{aligned} H_0 &= -2\,(n-1)^2\, h^3\, c \\ H_1 &= -(n-1)^2 h^2 f_3''(x_2, x_2) + 4\,(n-1)\,(n-2)\, h\,(b^2 - a\,c)\, x_1. \end{aligned}$$

Die durch die Gleichung $H = 0$ dargestellte Curve heisst die Hesse'sche Curve der Curve f. Die Formeln (2) und (3) zeigen, dass die Hesse'sche Curve dann und nur dann durch den Punkt ξ_3 hindurchgeht, wenn $H_0 = 0$, also $c = 0$, d. h. nach §. 86, wenn dieser Punkt ein Wendepunkt ist. Aus dem Ausdrucke für H_1 kann man noch weiter schliessen, dass die Wendetangente $x_1 = 0$ dann und nur dann zugleich Tangente der Curve $H = 0$ ist, wenn $f_3''(x_2, x_2)$ und folglich auch f_3 selbst durch x_1 theilbar ist. In diesem Falle wäre, wie aus (3) hervorgeht, $x_1 = 0$ eine im Punkte ξ_3 vierpunktig berührende Tangente. Dieser Fall kann bei den Curven dritter Ordnung nur dann vorkommen, wenn f durch x_1 theilbar ist, also niemals bei einer irreduciblen Curve dritter Ordnung.

Die Hesse'sche Curve geht ausser durch die Wendepunkte noch durch die singulären Punkte der Curve f, was hier nicht weiter untersucht werden soll.

Wenn wir also unsere Betrachtungen auf Curven f ohne singulären Punkt beschränken, so können wir sagen, dass jeder Schnittpunkt der Curve f mit ihrer Hesse'schen Curve einen Wendepunkt der Curve f giebt, und dass diese Curve f keine anderen Wendepunkte hat. Wenn Punkte mit vierpunktig berührender Tangente vorkommen, so berühren sich die Curven f und H, und wir können solche Punkte auffassen als durch das Zusammenfallen von zwei Wendepunkten entstanden. Wenden wir noch das Theorem von Bezout (Bd. I, §. 49) an, so erhalten wir das Ergebniss:

Eine Curve n^{ter} Ordnung ohne singulären Punkt hat $3n\,(n-2)$ Inflexionspunkte;

und speciell:

Eine Curve dritter Ordnung ohne singulären Punkt hat neun getrennt liegende Inflexionspunkte.

§. 89.

Inflexionspunkte einer Curve dritter Ordnung.

Es sei jetzt $f = 0$ die Gleichung einer Curve dritter Ordnung ohne singulären Punkt. Wir legen zwei der Ecken des Coordinatendreiecks ξ_1, ξ_2 in zwei von den neun Inflexionspunkten und nehmen die entsprechenden Inflexionstangenten für die Seiten x_2, x_1. Dann muss sich f, wenn $x_1 = 0$ oder $x_2 = 0$ gesetzt wird, auf das Glied $h x_3^3$ reduciren, worin h eine Constante ist, und folglich müssen alle Glieder, die in der cubischen Form einen von Null verschiedenen Coëfficienten haben, ausgenommen $h x_3^3$, durch $x_1 x_2$ theilbar sein. Demnach erhält f die Form

$$(1) \qquad f(x_1, x_2, x_3) = x_1 x_2 (a_1 x_1 + a_2 x_2 + a_3 x_3) + h x_3^3,$$

worin a_1, a_2, a_3 Constanten sind. Daraus aber geht hervor, dass die gerade Linie

$$a_1 x_1 + a_1 x_2 + a_3 x_3 = 0$$

gleichfalls Inflexionstangente der Curve f ist, und dass ihr Schnittpunkt mit der Linie $x_3 = 0$ ein dritter Inflexionspunkt ist. Dieser Punkt ist von den beiden ersten ξ_1, ξ_2 verschieden, weil weder a_1 noch $a_2 = 0$ sein kann, wenn die Curve keinen singulären Punkt hat. Wir wollen dieses wichtige Resultat in Form eines Satzes aussprechen:

1. Wenn man irgend zwei Inflexionspunkte einer Curve dritter Ordnung ohne singulären Punkt durch eine gerade Linie verbindet, so schneidet diese gerade Linie die Curve in einem dritten Inflexionspunkte.

Da es neun Inflexionspunkte giebt, so gehen von jedem dieser Punkte vier gerade Linien aus, deren jede noch zwei weitere Inflexionspunkte enthält. Es giebt neun solcher Büschel von vier Geraden, und weil jede dieser Geraden in drei Büscheln vorkommt, so ist die Anzahl der Geraden $9 . 4 : 3 = 12$. Wir können demnach den Satz 1. so ergänzen:

2. Die neun Inflexionspunkte einer Curve dritter Ordnung liegen zu je dreien auf zwölf geraden Linien, und durch jeden Inflexionspunkt gehen vier von diesen Geraden.

Aus dem Ausdruck (1) können wir eine **canonische Darstellung** für die cubische Form f herleiten:

Wir bezeichnen mit ε eine imaginäre dritte Einheitswurzel und führen zwei Variable z_1, z_2 ein, die durch die Gleichungen

$$(2) \qquad \begin{aligned} a_1 x_1 &= \varepsilon z_1 + \varepsilon^2 z_2 - {}^1\!/_3\, a_3 x_3 \\ a_2 x_2 &= \varepsilon^2 z_1 + \varepsilon z_2 - {}^1\!/_3\, a_3 x_3 \end{aligned}$$

definirt sind, woraus noch folgt:

$$(3) \qquad -(a_1 x_1 + a_2 x_2 + a_3 x_3) = z_1 + z_2 - {}^1\!/_3\, a_3 x_3.$$

Die Variablen z_1, z_2 sind durch (2) als lineare Functionen von x_1, x_2, x_3 bestimmt, und die linearen Functionen z_1, z_2, x_3 sind als Functionen von x_1, x_2, x_3 linear unabhängig. Wenn wir (2) und (3) in (1) einführen, so ergiebt sich

$$-a_1 a_2 f = z_1^3 + z_2^3 - \left(a_1 a_2 h + \frac{a_3^3}{27}\right) x_3^3 + a_3 z_1 z_2 x_3.$$

Diesem Ausdrucke giebt man eine mehr symmetrische Gestalt, indem man für z_1, z_2, x_3 drei neue lineare Functionen y_1, y_2, y_3 einführt, die sich von diesen nur um constante Factoren unterscheiden:

$$f = \varphi(y_1, y_2, y_3) = \alpha_1 y_1^3 + \alpha_2 y_2^3 + \alpha_3 y_3^3 + 6\, m\, y_1 y_2 y_3,$$

worin α_1, α_2, α_3, m Constanten bedeuten.

Wenn kein singulärer Punkt vorhanden ist, so können die Coëfficienten α_1, α_2, α_3 nicht verschwinden, und man kann sie ohne Beschränkung der Allgemeinheit einander gleich, etwa $= h$, annehmen. Man könnte sie sogar $= 1$ setzen, was aber, um die Homogeneïtät aufrecht zu erhalten, zunächst besser nicht geschieht. Wir haben also die **canonische Form** für die ternäre cubische Form:

$$(4) \qquad \varphi(y_1, y_2, y_3) = h(y_1^3 + y_2^3 + y_3^3) + 6\, m\, y_1 y_2 y_3.$$

Nach unserem Ausgangspunkte war die Linie x_3, oder was dasselbe ist, y_3 die Verbindungslinie dreier Inflexionspunkte. Solcher Linien giebt es aber zwölf, und wir können daher die Linie y_3 auf zwölf Arten wählen. Setzen wir aber y_1 oder y_2 an Stelle von y_3, so bekommen wir dieselbe Darstellung in der canonischen Form, und es giebt also nur vier wesentlich verschiedene Arten dieser Darstellung (abgesehen von dem willkürlichen h), d. h. vier Arten, die Linien y_1, y_2, y_3 zu bestimmen. Wir haben daher den Satz:

3. **Eine ternäre cubische Form $f(x_1, x_2, x_3)$, deren Discriminante von Null verschieden ist, lässt sich auf vier verschiedene Arten in die canonische Form**

$$\varphi(y_1, y_2, y_3) = h(y_1^3 + y_2^3 + y_3^3) + 6m\, y_1 y_2 y_3$$

transformiren.

Da auf jeder der Linien $y_1 = 0$, $y_2 = 0$, $y_3 = 0$ drei Inflexionspunkte liegen, so ist das Problem der Inflexionspunkte wesentlich identisch mit dem der Transformation der cubischen Form f auf die canonische Form, mit dem wir uns zunächst beschäftigen wollen [1]).

§. 90.

Transformation der cubischen Form auf die canonische Form.

Um die Transformation der cubischen ternären Form auf die canonische Form durchzuführen, d. h. auf die Lösung gewisser algebraischer Gleichungen zurückzuführen, müssen wir zunächst die Covarianten für die canonische Form bilden.

Es sei also

$$\varphi(y) = h(y_1^3 + y_2^3 + y_3^3) + 6m\, y_1 y_2 y_3,$$

wofür wir zur Abkürzung auch setzen:

(1) $$\varphi(y) = h\, \Sigma y_1^3 + 6m\, y_1 y_2 y_3,$$

indem wir unter dem Zeichen Σ eine Summe über drei durch cyklische Vertauschung der Variablen y_1, y_2, y_3 aus dem ersten gebildete Glieder verstehen.

Die Hesse'sche Covariante wollen wir zur Vereinfachung der Formeln mit einem geeigneten numerischen Factor multipliciren, und demnach

(2) $$\Delta(x) = \frac{1}{6^3} \begin{vmatrix} f_{11}, f_{12}, f_{13} \\ f_{21}, f_{22}, f_{23} \\ f_{31}, f_{32}, f_{33} \end{vmatrix}$$

---

1) Aus der Literatur über die Wendepunkte der Curven dritter Ordnung und über die Theorie der ternären cubischen Formen erwähnen wir ausser den älteren Arbeiten von Newton und MacLaurin: Hesse, „Ueber die Elimination etc." und „Ueber die Wendepunkte der Curven dritter Ordnung", Crelle's Journal, Bd. 28 (1844). Aronhold, Theorie der homogenen Functionen 3ten Grades von drei Veränderlichen, Crelle's Journal, Bd. 55 (1858). Salmon, Higher plane curves (deutsch von Fiedler).

setzen, worin f_{ik} für $f''(x_i, x_k)$ steht. Für die canonische Form erhält man hieraus durch einfache Rechnung

$$(3) \qquad \Delta(y) = -h m^2 \Sigma y_1^3 + (h^3 + 2 m^3)\, y_1 y_2 y_3.$$

Daraus leiten wir die zweite Covariante C_1 (§. 87) her, in der wir gleichfalls einen numerischen Factor einführen, und demnach

$$(4) \qquad J(x) = \frac{1}{36} \begin{vmatrix} f_{11}, f_{12}, f_{13}, \Delta_1 \\ f_{21}, f_{22}, f_{23}, \Delta_2 \\ f_{31}, f_{32}, f_{33}, \Delta_3 \\ \Delta_1, \Delta_2, \Delta_3, 0 \end{vmatrix}$$

setzen, worin Δ_i für $\Delta'(x_i)$ steht. Auch diese Covariante muss in der canonischen Form dargestellt werden, was keine Schwierigkeit hat, wenn man die Determinante nach der Formel Bd. I, §. 23, (12) bildet. Man findet so:

$$(5) \qquad \begin{aligned} J(y) = &- h^2 (h^3 + 8 m^3)^2 \Sigma y_2^3 y_3^3 \\ &+ 3 m^2 (5 h^6 + 26 h^3 m^3 - 4 m^6)\, y_1^2 y_2^2 y_3^2 \\ &+ h m (2 h^6 + 5 h^3 m^3 + 20 m^6)\, y_1 y_2 y_3 \Sigma y_1^3 \\ &+ 9 h^2 m^6 (\Sigma y_1^3)^2. \end{aligned}$$

Danach lassen sich die drei symmetrischen Functionen $y_1 y_2 y_3$, Σy_1^3, $\Sigma y_2^3 y_3^3$ durch die drei Formen $\varphi(y)$, $\Delta(y)$, $J(y)$, und also auch durch die entsprechenden Formen in den ursprünglichen Variablen x, die wir kurz durch f, Δ, J bezeichnen, nach den Invarianten-Relationen

$$(6) \qquad \varphi(y) = f, \quad \Delta(y) = r^2 \Delta, \quad J(y) = r^6 J$$

ausdrücken. Man erhält zunächst aus (1) und (3):

$$(7) \qquad (h^3 + 8 m^3)\, y_1 y_2 y_3 = m^2 f + r^2 \Delta,$$

$$(8) \qquad h (h^3 + 8 m^3) \Sigma y_1^3 = (h^3 + 2 m^3) f - 6 m r^2 \Delta,$$

und sodann aus (5)

$$(9) \qquad \begin{aligned} &h^2 (h^3 + 8 m^3)^2 \Sigma y_2^3 y_3^3 = \\ &(2 h^3 + m^3) m^3 f^2 + m (2 h^3 - 5 m^3) r^2 f \Delta + 3 m^2 r^4 \Delta^2 - r^6 J. \end{aligned}$$

Sehr einfach ist nun die Berechnung der dritten Covariante C_2 (§. 87) für die canonische Form.

Wir führen auch hier einen vereinfachenden numerischen Factor ein, und setzen

$$(10) \qquad K = K(x) = \frac{1}{9} \begin{vmatrix} f_1, \Delta_1, J_1 \\ f_2, \Delta_2, J_2 \\ f_3, \Delta_3, J_3 \end{vmatrix},$$

worin f_k, Δ_k, J_k die Ableitungen nach x_k bedeuten. Für die canonische Form ist dann

(11) $$K(y) = r^9 K.$$

Um $K(y)$ zu finden, brauchen wir nur die Functionaldeterminante aus den linken Theilen der Formeln (7), (8), (9) zu bilden, woraus sich mit Anwendung einfacher Determinantensätze ergiebt (Bd. I, §. 22, §. 27):

$$K(y) = -h^3(h^3 + 8m^3)^3 \begin{vmatrix} 1, & y_1^3, & y_1^6 \\ 1, & y_2^3, & y_2^6 \\ 1, & y_3^3, & y_3^6 \end{vmatrix},$$

und mithin ist

(12) $$r^9 K = h^3(h^3 + 8m^3)^3 (y_1^3 - y_2^3)(y_1^3 - y_3^3)(y_2^3 - y_3^3).$$

Zu bemerken ist noch zu diesen Formeln, dass der in ihnen auftretende Factor $h^3 + 8m^3$ nicht verschwinden kann, wenn die Curve f keinen singulären Punkt hat. Denn ein singulärer Punkt wird bestimmt durch die drei Gleichungen:

$$h y_1^2 + 2m y_2 y_3 = 0,\quad h y_2^2 + 2m y_3 y_1 = 0,\quad h y_3^2 + 2m y_1 y_2 = 0,$$

und diese drei Gleichungen sind mit einander verträglich, wenn $h^3 + 8m^3 = 0$. (Ist z. B. $h = -2m$, so sind sie befriedigt, wenn $y_1 = y_2 = y_3$ ist.)

Der Coëfficient h kann für eine gegebene Form f jeden vorgeschriebenen von Null verschiedenen Werth haben, und erst wenn dieser Werth gegeben ist, ist das Problem bestimmt. Wir wollen der Einfachheit halber jetzt $h = 1$ setzen, und erhalten aus (7) bis (9) das Resultat:

Setzt man

$$P = \frac{(2 + m^3) m^3 f^2 + (2 - 5m^3) m r^2 f \Delta + 3 m^2 r^4 \Delta^2 - r^6 J}{(1 + 8m^3)^2},$$

(13) $$Q = \frac{(1 + 2m^3) f - 6 m r^2 \Delta}{1 + 8m^3},$$

$$R = \frac{m^2 f + r^2 \Delta}{1 + 8m^3},$$

so sind y_1^3, y_2^3, y_3^3 die Wurzeln der cubischen Gleichung

(14) $$u^3 - Q u^2 + P u - R^3 = 0,$$

und die Discriminante dieser cubischen Gleichung ist:

Die Coëfficienten der cubischen Gleichung sind bekannt, sobald m^3, $m r^2$, r^6, oder auch, wenn m und r^3 bekannt sind.

Ist dann die Gleichung (14) gelöst, so sind y_1, y_2, y_3 bis auf dritte Einheitswurzeln, die aber der Relation $y_1\, y_2\, y_3 = R$ genügen müssen, bestimmt, und weiter können auch diese Grössen der Natur der Sache nach nicht bestimmt werden.

Wenn die Curve f eine reelle Curve ist, so ergiebt sich aus den Formeln (13) und (15) noch der Satz, dass, wenn m und r reell sind, D_1 positiv ist, und folglich die Wurzeln der Gleichung (14) alle drei reell sind.

Drückt man die Discriminante D_1 durch die Coëfficienten der Gleichung P, Q, R aus, so fliesst aus der Formel (15) noch das Resultat, dass man das Quadrat der Covariante K als ganze rationale Function der Covarianten f, $\varDelta$, J ausdrücken kann. Der Ausdruck wird ziemlich complicirt und soll hier nicht weiter verfolgt werden.

Um aber die biquadratische Gleichung zu bilden, von der m und r abhängen, ist es nöthig, auf die Invarianten dritter Ordnung näher einzugehen.

§. 91.

Die Invarianten der Curve dritter Ordnung und die biquadratische Gleichung.

Alle Curven dritter Ordnung, deren Gleichung in der canonischen Form durch dieselben Grössen $\Sigma\, y_1^3$, $y_1\, y_2\, y_3$ linear dargestellt werden kann, haben dieselben Punkte zu Wendepunkten, beispielsweise also die Curven $f = 0$ und $\varDelta = 0$, und allgemeiner alle Curven der Schaar

$$F = \lambda f + 6 \mu \varDelta = 0, \tag{1}$$

wo λ, μ beliebige Parameter sind. Alle Curven dieser Schaar schneiden sich in neun festen Punkten, und eine solche Schaar wird ein Curvenbüschel genannt. Die neun festen Punkte, die für alle Curven des Büschels die Wendepunkte sind, heissen die Grundpunkte. Bilden wir von der Form F die Hesse'sche Determinante, so wird auch diese Form linear durch $\Sigma\, y_1^3$ und $y_1\, y_2\, y_3$ ausgedrückt und kann daher nach §. 90, (7) und (8) auch linear durch f und $\varDelta$ ausgedrückt werden, d. h. wir erhalten eine Form desselben Büschels.

Wir setzen demnach diese Determinante

(2) $$\Delta_{\lambda,\mu}(x) = Lf + M\Delta,$$

worin L und M binäre Formen 3ten Grades von λ, μ sind.

Wenn wir eine beliebige lineare Transformation auf die Variablen x anwenden, so ist, wegen der Invarianten-Eigenschaft der Function Δ

(3) $$\Delta_{\lambda,\mu}(y,b) = r^2 \Delta_{\lambda,\mu r^2}(x,a),$$

und daraus folgt, dass die Coëfficienten der einzelnen Potenzen und Producte von λ, μ Covarianten der ursprünglichen Form sind, und die Coëfficienten L, M von f und Δ in diesen Ausdrücken, die rational von den Coëfficienten a der Form f abhängen, sind daher Invarianten dieser Form. Wir haben darin ein Mittel, diese Invarianten thatsächlich zu berechnen.

Bezeichnen wir nämlich mit a_i, A_i, B_i die Coëfficienten der einzelnen Potenzen und Producte der Variablen x in f, Δ und $\Delta_{\lambda,\mu}$, so ergiebt sich aus (2) ein System von zehn Gleichungen:

$$L a_i + M A_i = B_i,$$

woraus L und M bestimmt werden können. Man erhält, wenn i, k zwei verschiedene Indices sind,

(4) $$\begin{aligned} L\,(a_i A_k - a_k A_i) &= \quad B_i A_k - B_k A_i \\ M\,(a_i A_k - a_k A_i) &= - B_i a_k + B_k a_i. \end{aligned}$$

Daraus schliesst man noch, dass L, M ganze Functionen der Coëfficienten a_i sind. Denn in (4) sind die rechten Seiten ganze Functionen, und wenn also L oder M, in der einfachsten Gestalt dargestellt, noch einen Nenner hätten, so müssten die sämmtlichen Determinanten $a_i A_k - a_k A_i$, welches ganze Functionen 4ten Grades der a sind, einen gemeinschaftlichen Theiler haben. Dass dies aber nicht möglich ist, kann man an irgend einem speciellen Falle nachweisen, z. B. an der Form

$$f = 3x_3(\alpha x_1^2 + \beta x_2^2) + a x_1^3 + b x_2^3,$$

deren Hesse'sche Form:

$$-\beta^2(\alpha x_3 + a x_1)\,x_2^2 - \alpha^2(\beta x_3 + b x_2)\,x_1^2$$

ist. Hier kommen unter den $a_i A_k - a_k A_i$ z. B. die beiden Functionen $a^2\beta^2$, $b^2\alpha^2$ vor, die keinen gemeinschaftlichen Theiler haben.

Um $\Delta_{\lambda,\mu}$ für die canonische Form zu berechnen, hat man in §. 90, (3):

$$\text{durch} \quad \begin{matrix} h, & m \\ h(\lambda - 6m^2\mu), & m\lambda + (h^3 + 2m^3)\mu \end{matrix}$$

zu ersetzen, und man findet so:

$$\Delta_{\lambda,\mu} = -h(\lambda - 6m^2\mu)[m\lambda + (h^3 + 2m^3)\mu]^2 \Sigma y_1^3$$
$$+ \{h^3(\lambda - 6m^2\mu)^3 + 2[m\lambda + (h^3 + 2m^3)\mu]^3\} y_1 y_2 y_3,$$

woraus nach §. 90, (7), (8) mit Rücksicht auf (2) nach einigen einfachen Rechnungen folgt:

$$(5) \quad \begin{aligned} L &= -2\lambda^2\mu(h^3 - m^3)m - \lambda\mu^2(h^6 - 20h^3m^3 - 8m^6) \\ &\quad + 8\mu^3m^2(h^3 - m^3)^2, \\ M &= \lambda^3 + 12\lambda\mu^2 m(h^3 - m^3) + 2\mu^3(h^6 - 20h^3m^3 - 8m^6). \end{aligned}$$

Man bekommt also auf diese Weise nur zwei Invarianten vom 4ten und 6ten Grade, nämlich in der canonischen Form:

$$(6) \qquad m(h^3 - m^3), \quad h^6 - 20h^3m^3 - 8m^6.$$

Das Gewicht dieser Invarianten ist [nach Bd. I, §. 60, (3)] gleichfalls 4 und 6, und wenn wir sie also in der allgemeinen Form mit S und T bezeichnen und $h = 1$ setzen, so findet sich

$$(7) \quad \begin{aligned} m(1 - m^3) &= r^4 S, \\ 1 - 20m^3 - 8m^6 &= r^6 T. \end{aligned}$$

Für L und M erhält man aus (5) die Darstellung:

$$(8) \quad \begin{aligned} L &= -2S\lambda^2\mu - T\lambda\mu^2 + 8S^2\mu^3 \\ M &= \lambda^3 + 12S\lambda\mu^2 + 2T\mu^3. \end{aligned}$$

Die Functionen S und T vom 4ten und 6ten Grade sind zuerst von Aronhold berechnet worden. Wir wollen die langen Ausdrücke nicht hierher setzen, betrachten aber diese beiden Grössen jetzt als bekannt und gegeben.

Aus (7) lässt sich eine biquadratische Gleichung ableiten für das Verhältniss $m^2 : r^2$. Man findet nämlich daraus:

$$(9) \quad \begin{aligned} m^5 - m^8 &= r^4 m^4 S \\ m^2 - 2m^5 + m^8 &= r^8 S^2 \\ m^2 - 20m^5 - 8m^8 &= r^6 m^2 T. \end{aligned}$$

Wenn man daraus m^2 und m^5 eliminirt, so findet man

$$(10) \qquad 27m^8 + 18Sm^4r^4 + Tm^2r^6 - S^2r^8 = 0.$$

Diese Gleichung erhält eine einfachere Gestalt durch die Substitution

(11) $$z = \frac{3\,m^2}{r^2}.$$

Sie wird dann

(12) $$z^4 + 6\,S z^2 + T z - 3\,S^2 = 0.$$

Diese biquadratische Gleichung hat die Eigenschaft, dass ihre erste Invariante $A = 0$ ist, und dass ihre Discriminante (Bd. I, §. 47):

(13) $$D_2 = -27\,(T^2 + 64\,S^3)^2 = -27\,D^2,$$

also stets negativ ist. Die Grösse $D = T^2 + 64\,S^3$ erhält für die canonische Form (5) den Ausdruck:

(14) $$h^3\,(h^3 + 8\,m^3)^3,$$

und kann also nicht verschwinden, so lange die Curve f keinen singulären Punkt hat. (Sie ist in der That nichts Anderes, als die Discriminante der Form f.)

Aus (13) ergiebt sich nun, dass die biquadratische Gleichung (12) bei reellen Curven f eine negative Discriminante, und folglich (Bd. I, §. 78) zwei reelle und zwei conjugirt imaginäre Wurzeln hat, und weil das Product aller vier Wurzeln $-3\,S^2$ negativ ist, so ist von den reellen Wurzeln eine positiv, eine negativ.

Aus z kann man mit Hülfe von (11) und der ersten Gleichung (7) die beiden Grössen m und r berechnen. Man erhält so

(15) $$m^3 = \frac{z^2}{9\,S + z^2},\quad m\,r^2 = \frac{3\,z}{9\,S + z^2},\quad r^6 = \frac{27\,z}{(9\,S + z^2)^2},$$

und hier könnte, wie man aus (12) schliesst, wenn man $z^2 = -9\,S$ setzt, $9\,S + z^2$ nur dann verschwinden, wenn entweder S oder D Null ist. Damit sind die Coëfficienten P, Q, R^3 der cubischen Gleichung §. 90, (14) eindeutig durch z und durch bekannte Grössen bestimmt, und für die reelle positive Wurzel z wird m und r reell, und folglich auch y_1, y_2, y_3 reell.

Eine leichte Ausnahme bildet der Fall $S = 0$, in dem eine Wurzel der Gleichung (12) verschwindet, und die zweite reelle Wurzel $-\sqrt[3]{T}$ wird, und für die zugehörigen Werthe von m und r^6 erhält man aus (7) und (11)

$$m = 0,\ 1;\quad r^6 = \frac{1}{T},\ \frac{-27}{T};$$

je nachdem also T positiv oder negativ ist, fällt der erste oder der zweite Werth von r reell aus, und im Wesentlichen bleibt Alles wie vorher.

Es ergiebt sich hieraus der Satz:

Jede reelle ternäre cubische Form mit nicht verschwindender Discriminante kann durch eine reelle Transformation auf die reelle canonische Form gebracht werden.

Man kann jetzt leicht die Coordinaten der Wendepunkte in dem canonischen Coordinatensysteme angeben. Man erhält sie, wenn man in der Gleichung

$$y_1^3 + y_2^3 + y_3^3 + 6m\, y_1 y_2 y_3 = 0$$

je einmal $y_1, y_2, y_3 = 0$ setzt. Da eine der nicht verschwindenden Coordinaten $= 1$ gesetzt werden kann, so findet man, wenn ε eine imaginäre dritte Einheitswurzel ist, die folgenden Werthe der Coordinaten (y_1, y_2, y_3):

$$(16)\qquad \begin{array}{lll} (0,\, 1,\, -1), & (0,\, 1,\, -\varepsilon), & (0,\, 1,\, -\varepsilon^2), \\ (-1,\, 0,\, 1), & (-\varepsilon,\, 0,\, 1), & (-\varepsilon^2,\, 0,\, 1), \\ (1,\, -1,\, 0), & (1,\, -\varepsilon,\, 0), & (1,\, -\varepsilon^2,\, 0), \end{array}$$

und es folgt daraus, dass immer drei der Inflexionspunkte reell und sechs imaginär sind.

In der Tabelle (16) liegen je drei in einer Zeile stehende Punkte auf einer Geraden, nämlich auf den Geraden

$$y_1 = 0, \quad y_2 = 0, \quad y_3 = 0.$$

Es ist danach leicht, auch die übrigen Tripel von Punkten zusammenzustellen, die auf einer geraden Linie liegen, und damit diese zwölf Linien zu bestimmen. Man hat dabei nur immer solche Punkte zusammenzustellen, deren Coordinaten eine verschwindende Determinante geben. Man kann diese zwölf Linien auf vier Arten in Tripel anordnen, so dass in jedem Tripel alle neun Inflexionspunkte vorkommen. Das erste dieser Tripel wird von den Zeilen von (16) gebildet. Die drei anderen lauten so:

$$(17)\qquad \begin{array}{lll} (0,\, 1,\, -1), & (-1,\, 0,\, 1), & (1,\, -1,\, 0), \\ (0,\, 1,\, -\varepsilon), & (-\varepsilon,\, 0,\, 1), & (1,\, -\varepsilon,\, 0), \\ (0,\, 1,\, -\varepsilon^2), & (-\varepsilon^2,\, 0,\, 1), & (1,\, -\varepsilon^2,\, 0), \end{array}$$

$$
(18)\qquad \begin{matrix} (0,\ 1,\ -1), & (-\varepsilon,\ 0,\ 1), & (1,\ -\varepsilon^2,\ 0) \\ (-1,\ 0,\ 1), & (1,\ -\varepsilon,\ 0), & (0,\ 1,\ -\varepsilon^2) \\ (1,\ -1,\ 0), & (0,\ 1,\ -\varepsilon), & (-\varepsilon^2,\ 0,\ 1), \end{matrix}
$$

$$
(19)\qquad \begin{matrix} (0,\ 1,\ -1), & (-\varepsilon^2,\ 0,\ 1), & (1,\ -\varepsilon,\ 0) \\ (-1,\ 0,\ 1), & (1,\ -\varepsilon^2,\ 0), & (0,\ 1,\ -\varepsilon) \\ (1,\ -1,\ 0), & (0,\ 1,\ -\varepsilon^2), & (-\varepsilon,\ 0,\ 1). \end{matrix}
$$

Von den geraden Linien (16) enthält jede einen reellen und zwei conjugirt imaginäre Punkte, und alle drei Linien sind reell. Von den Geraden (17) enthält die erste die drei reellen Punkte und ist reell, während die beiden anderen conjugirt imaginär sind. In (18) und (19) sind alle drei Linien imaginär, und zwar sind die Linien von (18) conjugirt zu den Linien von (19).

Eine noch übersichtlichere Bezeichnung ist folgende. Wenn ξ und η je ein volles Restsystem nach dem Modul 3 durchlaufen, etwa 0, 1, 2, und zwei nach dem Modul 3 congruente Zahlen als nicht verschieden angesehen werden, so giebt es neun Combinationen (ξ, η), die wir als Bezeichnung für die neun Wendepunkte benutzen können. Setzen wir fest, dass (ξ, η) und (η, ξ) conjugirt imaginäre Wendepunkte, also (0, 0), (1, 1), (2, 2) die drei reellen bedeuten, so erhalten wir aus (16) bis (19) folgende Tabelle, in der wieder die in einer Zeile stehenden Wendepunkte auf einer geraden Linie liegen:

$$
(20)\qquad \begin{matrix} (0,0)\ (1,2)\ (2,1) & \quad & (0,0)\ (1,1)\ (2,2) \\ (1,1)\ (2,0)\ (0,2) & & (1,2)\ (2,0)\ (0,1) \\ (2,2)\ (0,1)\ (1,0) & & (2,1)\ (0,2)\ (1,0) \\ \\ (0,0)\ (2,0)\ (1,0) & & (0,0)\ (0,2)\ (0,1) \\ (1,1)\ (0,1)\ (2,1) & & (1,1)\ (1,0)\ (1,2) \\ (2,2)\ (1,2)\ (0,2) & & (2,2)\ (2,1)\ (2,0). \end{matrix}
$$

Man sieht hieraus, dass drei Wendepunkte (ξ_1, η_1), (ξ_2, η_2), (ξ_3, η_3) dann und nur dann auf einer geraden Linie liegen, wenn die beiden Congruenzen

$$
(21)\qquad \begin{matrix} \xi_1 + \xi_2 + \xi_3 \equiv 0 \\ \eta_1 + \eta_2 + \eta_3 \equiv 0 \end{matrix} \pmod 3
$$

erfüllt sind.

Man kann die Bezeichnung der vier Systeme von geraden Linien auch aus dem einen Schema:

(0, 0) (1, 2) (2, 1)
(1, 1) (2, 0) (0, 2)
(2, 2) (0, 1) (1, 0)

ableiten, wenn man die Zeilen, die Colonnen und die je drei den positiven und negativen Gliedern der Determinantenbildung entsprechenden Combinationen aufstellt.

§. 92.

Tripelgleichungen.

Das System der neun Wendepunkte hat die Eigenschaft, dass man aus zwei beliebigen von ihnen einen ganz bestimmten dritten auf rationalem Wege ableiten kann. Dies drückt sich als eine Eigenschaft der Gleichung 9ten Grades aus, von der die Bestimmung der Wendepunkte abhängt, die z. B. die Abscissen dieser Punkte zu Wurzeln hat. Wir stellen folgende Definition auf:

Eine Gleichung ohne gleiche Wurzeln heisst eine Tripelgleichung, wenn je zwei ihrer Wurzeln eine dritte bestimmen, so dass jede Wurzel eines solchen Tripels rational durch die beiden anderen ausgedrückt werden kann, und zwar so, dass man in einer Gleichung

(1) $$x_3 = \Theta(x_1, x_2),$$

in der Θ eine festgehaltene rationale Function bedeutet, für x_1, x_2, x_3 die Wurzeln irgend eines Tripels in beliebiger Reihenfolge setzen kann[1]).

Die Gleichung, von der die Wendepunkte abhängen, ist eine Tripelgleichung 9ten Grades. Es giebt aber auch Tripelgleichungen von anderem, z. B. vom 7ten Grade, zu denen die im vorigen Abschnitte betrachteten gehören[2]).

---

[1]) Die Tripelgleichungen 9ten Grades sind zuerst behandelt von Hesse in der Abhandlung: „Algebraische Auflösung derjenigen Gleichung 9ten Grades etc." in Crelle's Journal, Bd. 34 (1847).

[2]) Vgl. Nöther, Mathem. Annalen, Bd. 15 (1879): „Ueber die Gleichungen 8ten Grades und ihr Auftreten in der Theorie der Curven vierter Ordnung."

Wir wollen hier also nur auf die Tripelgleichungen 9ten Grades eingehen, und zunächst zeigen, wie sich aus der Tripeleigenschaft die Bezeichnung und Anordnung der Wurzeln ableiten lässt, die wir im vorigen Paragraphen für die Wendepunkte kennen gelernt haben.

Jede der neun Wurzeln kommt in vier Tripeln vor, und im Ganzen existiren daher $4.9:3=12$ verschiedene Tripel. Nehmen wir ein beliebiges von diesen Tripeln und bezeichnen dessen Wurzeln mit

$$(0, 0)\ (1, 2)\ (2, 1).$$

Dann sei (1, 1) eine beliebige vierte Wurzel. Diese bestimmt mit den drei ersten zunächst drei Tripel, die wir mit

$$(1, 1)\ (0, 0)\ (2, 2),\quad (1, 1)\ (1, 2)\ (1, 0),\quad (1, 1)\ (2, 1)\ (0, 1)$$

bezeichnen, und es bleiben noch zwei Wurzeln übrig, die das vierte Tripel mit (1, 1) bilden, und das wir nun mit

$$(1, 1)\ (2, 0)\ (0, 2)$$

bezeichnen.

Wir suchen nun das durch (0, 0), (2, 0) bestimmte Tripel. In diesem können keine Wurzeln vorkommen, die mit einer der beiden Wurzeln (0, 0), (2, 0) in einer der schon bestimmten Tripel vorkommen, also nicht

$$(1, 2)\ (2, 1)\ (1, 1)\ (2, 2)\ (0, 2),$$

und es bleibt für die dritte Wurzel dieses Tripels nur (0, 1) oder (1, 0) übrig, und dieselben beiden Wurzeln bleiben auch nur übrig für das durch (0, 0) (0, 2) bestimmte Tripel. Da wir aber noch (0, 2) mit (2, 0) vertauschen können, so beschränken wir die Allgemeinheit nicht, wenn wir die zwei weiteren Tripel

$$(0, 0)\ (2, 0)\ (1, 0),\quad (0, 0)\ (0, 2)\ (0, 1)$$

annehmen. Nun bestimmen wir die Tripel, die (1, 0) enthalten, von denen zwei schon bekannt sind. Die beiden anderen müssen die Wurzeln (2, 2), (0, 1), (0, 2), (2, 1) enthalten. Da aber (0, 1) (1, 0) (0, 2) und (0, 1) (1, 0) (2, 1) keine Tripel sind [weil (0, 1) (0, 2) das Tripel (0, 0) (0, 2) (0, 1) und (0, 1) (2, 1) das Tripel (1, 1) (2, 1) (0, 1) bestimmt], so haben wir die weiteren Tripel

$$(2, 2)\ (0, 1)\ (1, 0),\quad (1, 0)\ (0, 2)\ (2, 1).$$

Ebenso ergiebt sich

$$(0, 1)\ (2, 0)\ (1, 2).$$

Endlich bilden wir noch je ein (0, 2) und (2, 0) enthaltendes Tripel

$$(0, 2)\ (1, 2)\ (2, 2), \quad (2, 0)\ (2, 1)\ (2, 2),$$

womit alle zwölf Tripel, und damit die Anordnung §. 91, (20) bestimmt sind.

§. 93.

Die Gruppe der Tripelgleichungen.

Es soll nun die Galois'sche Gruppe P der Tripelgleichungen bestimmt werden. Zunächst ist klar, dass in dieser Gruppe nur solche Permutationen vorkommen, bei denen jedes Tripel wieder in ein Tripel übergeht. Denn nehmen wir an, die Wurzeln eines Tripels x_1, x_2, x_3 gehen durch eine Permutation in y_1, y_2, y_3 über, so folgt, da diese Permutation auf die Gleichung (1) (§. 92) anwendbar ist,

$$y_1 = \Theta\,(y_2, y_3),$$

und folglich ist y_1 die dritte Wurzel des durch y_2, y_3 bestimmten Tripels.

Gehen wir nun zu der Bezeichnung für die Wurzeln:

$$(1) \qquad x = (\xi, \eta)$$

über, so ergiebt sich aus der Zusammenstellung der Tripel in den §§. 91 und 92, dass drei Wurzeln

$$(2) \qquad x_1 = (\xi_1, \eta_1), \quad x_2 = (\xi_2, \eta_2), \quad x_3 = (\xi_3, \eta_3)$$

immer dann und nur dann ein Tripel bilden, wenn

$$(3) \qquad \begin{array}{l} \xi_1 + \xi_2 + \xi_3 \equiv 0 \\ \eta_1 + \eta_2 + \eta_3 \equiv 0 \end{array} \pmod 3.$$

Nennen wir eine Permutationsgruppe der (ξ, η), deren Substitutionen alle der vollständigen linearen Congruenzgruppe für den Modul 3 angehören (§. 78), eine **lineare Gruppe**, so gilt der Satz:

1. **Die Gruppe P einer Tripelgleichung ist immer linear.**

Nach §. 77 lässt sich jede Permutation der Grössen (ξ, η) überhaupt in der Form darstellen:

$$(4) \qquad \xi' \equiv \varphi\,(\xi, \eta), \quad \eta' \equiv \psi\,(\xi, \eta) \pmod 3,$$

worin φ, ψ ganze ganzzahlige Functionen der Variablen ξ, η sind, deren Grad in Bezug auf keine der Variablen den Werth 2 übersteigt. Ordnen wir diese Functionen nach η, so können wir setzen:

$$(5) \qquad \xi' = A\eta^2 + B\eta + C, \quad \eta' = A'\eta^2 + B'\eta + C',$$

worin A, B, C, A', B', C' ganze Functionen von ξ, höchstens vom 2ten Grade sind. Wir wollen in den Gleichungen (4) die Variable ξ festhalten und $\eta = 0, 1, 2$ setzen, d. h. wir wenden (5) auf das Tripel $(\xi, 0)$ $(\xi, 1)$ $(\xi, 2)$ an. Die entsprechenden (ξ_1', η_1'), (ξ_2', η_2'), (ξ_3', η_3') müssen dann den Relationen (3) genügen, also:

$$\begin{aligned} \xi_1' &\equiv C, & \eta_1' &\equiv C', \\ \xi_2' &\equiv A + B + C, & \eta_2' &\equiv A' + B' + C', \\ \xi_3' &\equiv A - B + C, & \eta_3' &\equiv A' - B' + C', \end{aligned}$$

und daraus folgt, dass A und A' für jedes ξ congruent mit Null sein müssen.

Ebenso kann man schliessen, dass in den Substitutionen (4) kein Glied mit ξ^2 vorkommen kann, und dass daher diese Substitutionen die Form haben müssen:

$$\left.\begin{aligned} \xi' &\equiv m\,\xi\eta + a\,\xi + b\,\eta + c \\ \eta' &\equiv m'\xi\eta + a'\xi + b'\eta + c' \end{aligned}\right\} \pmod 3.$$

Wenn man aber diese Substitutionen auf das Tripel (0, 0) (1, 1) (2, 2) anwendet, und die Summe der entsprechenden ξ' und η' gleich Null setzt, so folgt, dass $m = m' = 0$ sein muss, und dass also jede Permutation der Gruppe P in der Form

$$(6) \qquad \left.\begin{aligned} \xi' &\equiv a\,\xi + b\,\eta + c \\ \eta' &\equiv a'\xi + b'\eta + c' \end{aligned}\right\} \pmod 3$$

enthalten sein muss, wie behauptet war.

2. Umgekehrt gehen durch jede lineare Substitution von der Form (6) drei Grössen (ξ, η) eines Tripels in drei (ξ', η') über, die gleichfalls ein Tripel bilden.

Denn aus (6) folgt für irgend drei Zahlenpaare (ξ_1, η_1), (ξ_2, η_2), (ξ_3, η_3):

$$(7) \qquad \left.\begin{aligned} \xi_1' + \xi_2' + \xi_3' &\equiv a\,(\xi_1 + \xi_2 + \xi_3) + b\,(\eta_1 + \eta_2 + \eta_3) \\ \eta_1' + \eta_2' + \eta_3' &\equiv a'(\xi_1 + \xi_2 + \xi_3) + b'(\eta_1 + \eta_2 + \eta_3) \end{aligned}\right\} \pmod 3;$$

also wenn $\xi_1 + \xi_2 + \xi_3$ und $\eta_1 + \eta_2 + \eta_3$ mit Null congruent ist, so gilt dasselbe von den linken Seiten von (7).

Nun gehen auch umgekehrt durch jede lineare Substitution der Form (6) immer drei Grössen (ξ, η) eines Tripels in ein Tripel über, und daraus lässt sich beweisen, dass jede Gleichung 9ten Grades, deren Galois'sche Gruppe P in der vollständigen linearen Congruenzgruppe enthalten ist, eine Tripelgleichung ist, wenn noch die weitere Bedingung hinzukommt, dass durch die Gruppe P irgend zwei gegebene Wurzeln in zwei andere gleichfalls beliebig gegebene Wurzeln übergehen, oder, was damit gleichbedeutend ist, wenn P zweifach transitiv ist.

Denn wenn P aus lauter linearen Substitutionen besteht, so reducirt sich P durch Adjunction zweier beliebiger Wurzeln $x_1 = (\xi_1, \eta_1)$, $x_2 = (\xi_2, \eta_2)$ auf eine Gruppe P_1, die nicht nur x_1, x_2, sondern auch die dritte Wurzel $x_3 = (\xi_3, \eta_3)$ des durch x_1, x_2 bestimmten Tripels ungeändert lässt, und folglich gehört x_3 dem neuen Rationalitätsbereiche an, und mithin ist x_3 rational durch x_1, x_2 ausdrückbar in der Form

$$(8) \qquad x_3 = \Theta\,(x_1, x_2).$$

Wenn nun die Gruppe P zweifach transitiv ist, so giebt es eine Permutation in P, durch die x_1, x_2 in zwei beliebige andere Wurzeln y_1, y_2 übergehen, und durch die folglich auch x_3 in die dritte Wurzel des Tripels y_1, y_2, y_3 übergeht, und diese Permutation ist auf (8) anwendbar. Also ist auch

$$y_3 = \Theta\,(y_1, y_2).$$

Wir sprechen dies als Satz aus:

3. Jede Gleichung 9ten Grades, deren Gruppe linear und zweifach transitiv ist, ist eine Tripelgleichung.

Durch die Permutationen einer zweifach transitiven linearen Gruppe kann jedes Tripel in jedes andere, und zwar in beliebiger Anordnung, übergeführt werden.

Die Voraussetzung der zweifachen Transitivität kann auch so ausgedrückt werden, dass alle die Permutationen aus P, die eine Wurzel ungeändert lassen, die übrigen noch transitiv mit einander verbinden. Bezeichnen wir mit P_0 die in P enthaltene Gruppe, durch deren Permutationen eine der Wurzeln x_0 ungeändert bleibt, so muss P_0 in Bezug auf die anderen Wurzeln noch transitiv sein. Ist aber die Gruppe P nur einfach transitiv,

so ist P_0 nicht mehr transitiv, d. h. nach Adjunction von x_0 zerfällt die Gleichung für die übrigen acht Wurzeln in mehrere Factoren. Wenn die Gruppe P überhaupt transitiv ist, so kann hierbei x_0 jede beliebige der Wurzeln sein; denn wenn π eine Permutation von P ist, durch die x_0 in x_1 übergeht, so bleibt durch $P_1 = \pi^{-1} P_0 \pi$ die Wurzel x_1 ungeändert, und wenn P_0 für acht Wurzeln intransitiv ist, so muss auch P_1 für acht Wurzeln intransitiv sein, da sich die Permutationen von P_1 von denen von P_0 nur durch die Bezeichnung der Wurzeln unterscheiden (Bd. I, §. 154, 6.).

Die einfach transitiven unter den linearen Gruppen haben einen specielleren Charakter als die Gruppe der Tripelgleichungen.

Wir haben im §. 78 eine Zerlegung der allgemeinen linearen Congruenzgruppe für den Modul 3 kennen gelernt, an der wir diese Verhältnisse übersehen können.

Die Abel'sche Gruppe Q, die aus den Substitutionen

(9) $$\xi' \equiv \xi + \alpha, \quad \eta' \equiv \eta + \beta \pmod 3$$

besteht, ist gewiss nur einfach transitiv; denn wenn eine Wurzel durch (9) ungeändert bleiben soll, so muss $\alpha \equiv 0$, $\beta \equiv 0$ sein und alle Wurzeln bleiben ungeändert. Jede Wurzel ist rational durch jede andere ausdrückbar.

Suchen wir nun in der Gruppe P die Gruppe P_0 der Substitutionen auf, durch die (0, 0) ungeändert bleibt, so enthält P_0 nur homogene Substitutionen und ist also der grösste gemeinschaftliche Theiler von P und der homogenen Congruenzgruppe S, und es ist $P = P_0\, Q$.

Bilden wir für S die Compositionsreihe (§. 78):

$$S,\ S_1,\ S_2,\ S_3,\ S_4,$$

so ist $S_4 = \begin{pmatrix} 1, 0 \\ 0, 1 \end{pmatrix}, \begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}$, und durch S_4 gehen die Wurzeln (1, 1), (2, 2) nur in einander über. Durch $S_4\, Q$ kann das Tripel (0, 0) (1, 1) (2, 2) zwar jede Anordnung seiner Wurzeln erfahren. Es kann aber nur noch in die beiden anderen Tripel (1, 0) (2, 1) (0, 2); (0, 1) (1, 2) (2, 0) übergehen. $S_4\, Q$ ist also nur einfach transitiv und ist überdies imprimitiv.

Durch die Gruppe S_3, die aus S_4 durch Hinzunahme der Substitution

$$\begin{pmatrix} -1, 1 \\ 1, 1 \end{pmatrix}$$

entsteht, kann (1, 1), (2, 2) noch in (0, 2), (0, 1), aber nicht in (2, 0), (1, 0) oder in (1, 2), (2, 1) übergehen. Also ist auch die Gruppe $S_3 Q$ noch nicht zweifach transitiv, wohl aber ist sie primitiv. Nehmen wir aber, um S_2 zu bilden, noch die Substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$

hinzu, so geht (1, 1), (2, 2) in (0, 2), (0, 1) und in (1, 2), (2, 1) und (2, 0), (1, 0) über. Also ist die Gruppe $S_2 Q$ zweifach transitiv und folglich auch $S_1 Q$ und $S Q$. Es fangen also erst bei $S_2 Q$ die Tripelgleichungen an. Die Gleichungen mit engeren Gruppen sind noch keine eigentlichen Tripelgleichungen.

Wir können noch andere in $S Q$ enthaltene lineare Gruppen bilden, z. B. wenn wir mit S' die cyklische Gruppe 3ten Grades:

$$S' = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}, \begin{pmatrix} 1, & 0 \\ -1, & 1 \end{pmatrix}$$

bezeichnen, die Gruppe 27sten Grades $S' Q = Q S'$. Durch die Gruppe S' geht (1, 1) (2, 2) in (1, 1) (2, 2), (1, 2) (2, 1), (1, 0) (2, 0) über, während (0, 1) (0, 2) nicht daraus entsteht. Also ist auch dies nicht die Gruppe einer Tripelgleichung.

Hier wäre noch ein Feld weitergehender Untersuchungen über diese speciellen metacyklischen Gleichungen 9ten Grades und die Darstellung ihrer Wurzeln nach den Principien von Kronecker (Bd. I, achtzehnter Abschnitt).

§. 94.

Realitätsverhältnisse der Tripelgleichungen.

Wenn der Rationalitätsbereich reell ist, so können wir über die Realität der Wurzeln einer Tripelgleichung 9ten Grades einige allgemeine Schlüsse machen. Wenn in diesem Falle nämlich in einem Tripel zwei reelle Wurzeln vorkommen, so muss, wie aus der Gleichung $x_3 = \Theta(x_1, x_2)$ folgt, auch die dritte Wurzel reell sein. Wenn also überhaupt eine imaginäre Wurzel vorhanden ist, so muss in jedem der vier Tripel, dem diese Wurzel angehört, mindestens noch eine zweite imaginäre Wurzel vorkommen, und folglich ist die Anzahl der imaginären Wurzeln mindestens gleich 5, oder, da die Zahl der imaginären Wurzeln

gerade sein muss, gleich 6. Zwei reelle oder zwei conjugirt imaginäre Wurzeln x_1, x_2 gehören immer einem Tripel an, dessen dritte Wurzel reell ist; dies ergiebt sich aus der Gleichung:

$$x_3 = \Theta(x_1, x_2) = \Theta(x_2, x_1).$$

Wir wollen demnach ein Tripel, was zwei reelle oder zwei conjugirt imaginäre Wurzeln enthält, ein reelles Tripel nennen. Wenn in einem Tripel irgend imaginäre Wurzeln vorkommen, so bilden auch die conjugirt imaginären Wurzeln ein Tripel, und zwei solche Tripel sollen conjugirt imaginäre Tripel heissen.

Es giebt dann drei Möglichkeiten:

1. Lauter reelle Wurzeln.

2. Eine reelle und acht imaginäre Wurzeln.

In diesem Falle müssen die vier Paare conjugirt imaginärer Wurzeln vier Tripel bestimmen, die alle dieselbe reelle Wurzel als dritte enthalten. Bezeichnen wir diese reelle Wurzel mit (0, 0), so müssen

$$(1,2)\ (2,1),\quad (1,1)\ (2,2),\quad (1,0)\ (2,0),\quad (0,1)\ (0,2)$$

die vier Paare conjugirter Wurzeln sein.

3. Drei reelle und sechs imaginäre Wurzeln.

Die drei reellen Wurzeln müssen hier ein Tripel bilden. Nehmen wir für die reellen Wurzeln

$$(1)\qquad (0,0)\ (1,1)\ (2,2),$$

so können in den beiden Reihen

$$(2)\qquad \begin{matrix} (1,2)\ (0,2)\ (1,0) \\ (2,1)\ (2,0)\ (0,1) \end{matrix}$$

conjugirt imaginäre Wurzeln nicht in derselben Reihe vorkommen, weil sonst die dritte Wurzel der betreffenden Reihe reell wäre.

Es ist zu zeigen, dass die durch die conjugirten Paare bestimmten drei reellen Tripel zusammen alle drei reellen Punkte enthalten müssen.

Nehmen wir nämlich an, unter den drei Tripeln

$$(0,0)\ (1,2)\ (2,1),\quad (0,0)\ (2,0)\ (1,0),\quad (0,0)\ (0,1)\ (0,2)$$

kommen zwei reelle vor, so muss auch das dritte reell sein, d. h. es müssen

$$(1,2)\ (2,1),\quad (2,0)\ (1,0),\quad (0,1)\ (0,2)$$

conjugirte Paare sein. Dann aber bilden die drei Wurzeln (1, 1) (2, 0) (0, 2) ein Tripel, deren conjugirte (1, 1) (1, 0) (0, 1) kein Tripel bilden, was unmöglich ist. Jede der drei reellen Wurzeln (0, 0), (1, 1), (2, 2) kommt also ausser in (1) noch in einem und nur in einem reellen Tripel vor, dessen beide anderen Wurzeln conjugirt imaginär sind, und der dritte Fall führt also zu der Anordnung der reellen und imaginären Wurzeln, die wir bei den Wendepunkten der Curve dritter Ordnung kennen gelernt haben.

Dass aber auch die Fälle 1. und 2. vorkommen können, lehrt folgende Betrachtung: Aus einer allgemeinen Gleichung 9ten Grades erhält man eine Tripelgleichung durch Adjunction einer zu der linearen Gruppe SQ gehörigen Function. Eine solche Function ist z. B.:

$$\begin{aligned} v = & (0,0)(1,1)(2,2) + (0,0)(1,2)(2,1) + (0,0)(1,0)(2,0) \\ & + (0,0)(0,1)(0,2) + (1,1)(1,2)(1,0) + (1,1)(2,1)(0,1) \\ & + (1,1)(0,2)(2,0) + (1,2)(0,1)(2,0) + (2,2)(2,1)(2,0) \\ & + (2,2)(1,2)(0,2) + (2,2)(0,1)(1,0) + (2,1)(0,2)(1,0), \end{aligned}$$

und diese Function ist reell in den Fällen 1., 2., 3. Also ist auch der erweiterte Rationalitätsbereich, in dem unsere Gleichung eine Tripelgleichung ist, reell.

Zwölfter Abschnitt.

Die Doppeltangenten einer Curve vierter Ordnung.

---

§. 95.

Anzahl der Doppeltangenten einer Curve vierter Ordnung.

Ein geometrisches Problem, das wegen seiner mannigfachen Beziehungen zu anderen Gebieten von besonderer Bedeutung ist, was zugleich in ähnlicher Weise, wie das Problem der Wendepunkte der Curven dritter Ordnung, merkwürdige algebraische Verhältnisse bietet, ist das der Doppeltangenten der Curven vierter Ordnung.

Unter einer Doppeltangente einer Curve versteht man, wie schon im §. 86 bemerkt ist, eine gerade Linie, die die Curve in zwei verschiedenen Punkten berührt. Bei Curven von niedrigerer als der vierten Ordnung können Doppeltangenten nicht auftreten.

Bei den Curven vierter Ordnung hat eine Doppeltangente ausser den Berührungspunkten keinen Punkt mit der Curve gemein. In besonderen Fällen können die beiden Berührungspunkte auch zusammenfallen. Dann haben wir Linien mit vierpunktiger Berührung.

Die Bestimmung der Doppeltangenten wird als algebraisches Problem von einer gewissen algebraischen Gleichung abhängen, deren Grad gleich der Anzahl der Doppeltangenten ist, und die erste Frage ist die nach dem Grade dieser Gleichung, also nach der Anzahl der Doppeltangenten. Wir beschränken uns hier auf die Betrachtung von Curven vierter Ordnung, obwohl der Weg, den wir gehen, auch auf Curven höherer Ordnung anwendbar

ist. Wir setzen auch voraus, dass die Curve vierter Ordnung frei von singulären Punkten sei [1]).

Es möge jetzt $f(x_1, x_2, x_3)$ oder kürzer $f(x)$ eine ternäre Form 4ten Grades sein, die, gleich Null gesetzt, eine Curve vierter Ordnung ohne singulären Punkt darstellt, die wir die Curve f nennen.

Setzen wir in dieser Gleichung

$$(1) \qquad f(x_1, x_2, x_3) = 0$$

an Stelle der Variablen x_1, x_2, x_3 Ausdrücke von der Form

$$x_1 + t y_1, \quad x_2 + t y_2, \quad x_3 + t y_3,$$

so ergiebt sich eine Gleichung 4ten Grades in Bezug auf t:

$$(2) \qquad f(x + t y) = 0,$$

deren Wurzeln, wenn (x) und (y) zwei feste Punkte sind, in $x + t y$ eingesetzt, die Coordinaten der Schnittpunkte der Verbindungslinie der Punkte (x), (y), die wir als die Linie (x, y) bezeichnen wollen, mit der Curve f geben.

Es werde nun die Function $f(x + t y)$ nach Potenzen von t geordnet. Dies giebt (nach Bd. I, §. 60):

$$(3) \qquad f(x+yt) = \\ P_0(x,y) + 4 t P_1(x,y) + 6 t^2 P_2(x,y) + 4 t^3 P_3(x,y) + t^4 P_4(x,y),$$

worin die $P_\nu(x, y)$ die Polaren von $f(x)$ sind, also homogene

---

[1]) Jacobi, „Ueber die Anzahl der Doppeltangenten ebener algebraischer Curven", Crelle's Journal, Bd. 40 (1850). Clebsch, „Bemerkung zu Jacobi's Beweis für die Anzahl der Doppeltangenten", ebend., Bd. 63 (1864). Aus der ziemlich umfassenden Literatur über die Theorie der Doppeltangenten einer Curve vierter Ordnung sind die folgenden Schriften hervorzuheben. Zunächst mehrere Arbeiten von Hesse in Crelle's Journal, Bd. 41, 49, 52. Ferner Steiner, Eigenschaften der Curven vierter Ordnung rücksichtlich ihrer Doppeltangenten, Crelle's Journal, Bd. 49. Aronhold, Monatsber. d. Berl. Akademie 1864. Geiser, „Ueber die Doppeltangenten einer ebenen Curve 4ten Grades", Math. Annalen, Bd. 1 (1868). Cayley, Crelle's Journal, Bd. 68 (1868). Auch das oben citirte Werk von Salmon ist hier hervorzuheben. In neuerer Zeit wurde die Theorie der Doppeltangenten im Zusammenhange mit der Theorie der Abel'schen Functionen weiter ausgebildet. Riemann, Gesammelte mathematische Werke (2. Aufl., 1892) XXXI, aus dem Nachlass. Weber, Theorie der Abel'schen Functionen vom Geschlecht 3, Berlin 1876. Frobenius, Crelle's Journal, Bd. 99 u. 103. Die algebraische Seite der Frage ist in zwei Abhandlungen: Nöther, Math. Annalen, Bd. 15 und Weber, ebend., Bd. 23 behandelt.

Functionen ν^{ter} Ordnung in Bezug auf y, und $(4-\nu)^{\text{ter}}$ Ordnung in Bezug auf x. Es ist nämlich

$$
(4) \qquad
\begin{aligned}
P_0(x, y) &= \quad f(x) \\
P_1(x, y) &= \tfrac{1}{4} \sum_i y_i f'(x_i) \\
P_2(x, y) &= \tfrac{1}{12} \sum_i y_i y_k f''(x_i x_k) \\
P_3(x, y) &= \tfrac{1}{4} \sum_i x_i f'(y_i) \\
P_4(x, y) &= \quad f(y).
\end{aligned}
$$

Wenn x auf der Curve f liegt, so wird $P_0 = 0$, und eine Wurzel der Gleichung (2) verschwindet. Nehmen wir ausserdem noch (y) auf der Tangente im Punkte (x) an, so ist auch $P_1(x, y) = 0$, und es verschwinden zwei Wurzeln von (2). Die beiden übrigen werden nach (3) durch die quadratische Gleichung

$$
(5) \qquad 6 P_2 + 4 t P_3 + t^2 P_4 = 0
$$

bestimmt. Wenn diese Gleichung zwei gleiche Wurzeln hat, so wird die Linie (x, y) noch einen zweiten Berührungspunkt mit der Curve f haben, d. h. sie wird Doppeltangente sein. Die Bedingung hierfür ist aber die, dass die Discriminante der Gleichung (5) verschwindet, oder dass

$$
(6) \qquad R(x,y) = 2 P_3^2 - 3 P_4 P_2
$$

gleich Null sei. Hierin ist $R(x, y)$ eine in Bezug auf jedes der beiden Systeme (x) und (y) homogene Function, und zwar für die x vom 2ten, für die y vom 6ten Grade. Es ist aber noch zu bemerken, dass die Gleichung $R = 0$ auch dann erfüllt ist, wenn (x) ein beliebiger Punkt der Curve ist, und (y) mit (x) zusammenfällt, weil dann

$$
P_2(x,x) = P_3(x,x) = P_4(x,x) = f(x) = 0
$$

wird. Sonst aber wird R nur dann verschwinden, wenn die Linie (x, y) eine Doppeltangente ist. Wir stellen also den Satz auf:

1. Die Gleichung $R(x,y) = 0$ ist, wenn (x) ein Punkt der Curve f und (y) ein von (x) verschiedener Punkt der Tangente in (x) ist, die nothwendige und hinreichende Bedingung dafür, dass (x) ein Berührungspunkt einer Doppeltangente sei.

Es kommt nun darauf an, aus dieser Bedingung eine andere herzuleiten, die nur die x allein enthält, und die für keine

anderen Punkte als die Berührungspunkte der Doppeltangenten befriedigt ist.

Die Variablen y genügen der Tangentengleichung

$$(7) \qquad y_1 f'(x_1) + y_2 f'(x_2) + y_3 f'(x_3) = 0.$$

Bezeichnen wir mit b_1, b_2, b_3 irgend drei willkürliche Constanten, und setzen

$$(8) \qquad b_x = b_1 x_1 + b_2 x_2 + b_3 x_3,$$

so dass $b_x = 0$ die Gleichung einer willkürlichen geraden Linie ist, so können wir zu (7) noch die Gleichung

$$(9) \qquad b_1 y_1 + b_2 y_2 + b_3 y_3 = 0$$

hinzunehmen, also (y) als den Schnittpunkt der Tangente in (x) mit der beliebigen geraden Linie b_x auffassen. Dann erhalten wir

$$(10) \qquad \begin{aligned} y_1 &= b_2 f'(x_3) - b_3 f'(x_2), \\ y_2 &= b_3 f'(x_1) - b_1 f'(x_3), \\ y_3 &= b_1 f'(x_2) - b_2 f'(x_1), \end{aligned}$$

und hierdurch ist die Bedingung (7) identisch befriedigt. Durch diese Substitution geht $R(x, y)$ in eine homogene Function 20sten Grades der x und 6ten Grades der b über, die wir mit $D(x, b)$ bezeichnen wollen. Diese Function $D(x, b)$ verschwindet aber ausser in den Berührungspunkten der Doppeltangenten noch in den vier Schnittpunkten der Geraden b_x mit der Curve f. Diese Bedingung muss nun noch so umgeformt werden, dass sie von den b unabhängig wird.

Gehen wir von dem Punkte (y) zu einem beliebigen anderen Punkte der Tangente über, so können wir dies dadurch erreichen, dass wir y durch $\mu x + \lambda y$ ersetzen, worin λ, μ zwei willkürliche Parameter bedeuten. Dadurch geht $f(x + ty)$ in

$$f[(1 + \mu t) x + \lambda t y] = (1 + \mu t)^4 f\left(x + \frac{\lambda t}{1 + \mu t} y\right)$$

über, und die Entwickelung (3) ergiebt, wenn wir

$$P_0(x, y), \; P_1(x, y), \; P_1(x, \mu x + \lambda y)$$

gleich Null setzen:

$$\begin{aligned} & 6 t^2 (1 + \mu t)^2 \lambda^2 P_2(x, y) + 4 t^3 (1 + \mu t) \lambda^3 P_3(x, y) + t^4 \lambda^4 P_4(x, y) \\ &= 6 t^2 P_2(x, \mu x + \lambda y) + 4 t^3 P_3(x, \mu x + \lambda y) + t^4 P_4(x, \mu x + \lambda y). \end{aligned}$$

also, wenn wir beiderseits nach Potenzen von t ordnen:

$$P_2(x, \mu x + \lambda y) = \lambda^2 P_2(x, y)$$
$$P_3(x, \mu x + \lambda y) = 3\lambda^2 \mu P_2(x, y) + \lambda^3 P_3(x, y)$$
$$P_4(x, \mu x + \lambda y) = 6\lambda^2 \mu^2 P_2(x, y) + 4\lambda^3 \mu P_3(x, y) + \lambda^4 P_4(x, y),$$

und hieraus erhält man nach (6)

(11) $$R(x, \mu x + \lambda y) = \lambda^6 R(x, y).$$

Diese Formel gilt aber nicht identisch, sondern nur unter der Voraussetzung, dass (x) ein Punkt der Curve sei, also dass $f(x) = 0$ ist.

Der Punkt $(\mu x + \lambda y)$ kann ein ganz beliebiger Punkt der Tangente in (x) sein, und daher können wir, wenn a_1, a_2, a_3 drei willkürliche Grössen sind, über μ, λ so verfügen, dass

(12) $$\begin{aligned} \mu x_1 + \lambda y_1 &= a_2 f'(x_3) - a_3 f'(x_2) \\ \mu x_2 + \lambda y_2 &= a_3 f'(x_1) - a_1 f'(x_3) \\ \mu x_3 + \lambda y_3 &= a_1 f'(x_2) - a_2 f'(x_1) \end{aligned}$$

wird. Dann ist $(\mu x + \lambda y)$ der Schnittpunkt der Tangente mit der Geraden $a_x = 0$, wenn

(13) $$a_x = a_1 x_1 + a_2 x_2 + a_3 x_3$$

gesetzt ist. Dadurch geht $R(x, \mu x + \lambda y)$ in $D(x, a)$ über.

Um nun λ und μ zu bestimmen, multipliciren wir die Gleichungen (10) und (12) mit a_1, a_2, a_3, sodann (12) mit b_1, b_2, b_3 und addiren jedesmal. Dadurch erhalten wir mit Rücksicht auf $b_y = 0$:

$$a_y = -\mu b_x = \Sigma \pm a_1 b_2 f'(x_3)$$
$$\mu a_x + \lambda a_y = 0,$$

und daraus

$$\lambda b_x = a_x.$$

Hiernach lässt sich die Gleichung (11) so darstellen:

(14) $$\frac{D(x, a)}{a_x^6} = \frac{D(x, b)}{b_x^6},$$

und zeigt in dieser Form, dass der Quotient $D(x, a) : a_x^6$ von den willkürlichen Grössen a unabhängig ist. Die Gleichung (14) ist aber keine Identität, sondern sie ist nur befriedigt, so lange $f(x) = 0$ ist. Wir können aber eine Identität daraus herleiten, wenn wir annehmen, dass $f(x)$ irreducibel sei (oder wenigstens keinen mehrfach zählenden Factor enthält). Es ist nämlich die Form 26sten Grades

$$b_x^6 D(x, a) - a_x^6 D(x, b)$$

gleich Null für alle der Gleichung $f(x) = 0$ genügenden Werthe von (x), und folglich muss sie durch $f(x)$ theilbar sein. Wir können also, wenn wir mit $\Phi(x, a, b)$ eine Form 22sten Grades bezeichnen, setzen:

$$(15) \qquad b_x^6\, D(x, a) - a_x^6\, D(x, b) = f(x)\, \Phi(x, a, b).$$

Denken wir uns in (15) für einen Augenblick ein neues Coordinatensystem eingeführt, in dem die Linien a_x, b_x zwei Axen sind, von denen wir voraussetzen, dass sie sich nicht auf der Curve f schneiden, so folgt aus der Vergleichung der rechten und linken Seite der identischen Gleichung (15), dass in Φ kein Glied vorkommen kann, was nicht entweder mit a_x^6 oder mit b_x^6 multiplicirt ist, und folglich hat $\Phi(x)$ die Form

$$\Phi(x, a, b) = a_x^6\, \Phi_2(x) - b_x^6\, \Phi_1(x),$$

worin Φ_1, Φ_2 Formen 16ter Ordnung sind. Demnach erhält die identische Gleichung (15) die Form

$$b_x^6\, [D(x,a) + f(x)\, \Phi_1(x)] = a_x^6\, [D(x,b) + f(x)\, \Phi_2(x)],$$

und sie zeigt, dass $D(x, a) + f(x)\, \Phi_1(x)$ durch a_x^6 theilbar ist. Es existirt also eine Form 14ten Grades $\chi(x, a, b)$, so dass

$$(16) \qquad \frac{D(x, a)}{a_x^6} = \chi(x, a, b) - f(x)\, \frac{\Phi_1(x, a, b)}{a_x^6}.$$

Setzen wir hierin für die a und b irgend specielle, z. B. rationale Werthe c, d, und bezeichnen $\chi(x, c, d)$, was dann nur noch von x und von den Coëfficienten der Form $f(x)$ abhängig ist, mit $\chi(x)$, so folgt:

$$\frac{D(x, c)}{c_x^6} = \chi(x) - f(x)\, \frac{\Phi_1(x, c, d)}{c_x^6},$$

und wenn wir dies von (16) subtrahiren und die Relation (15) für $b = c$ benutzen:

$$(17) \qquad \chi(x, a, b) - \chi(x) = f(x)\, \Psi(x),$$

worin $\Psi(x)$ eine Function ist, die jedenfalls keinen anderen Nenner enthalten kann, als ein Product von Potenzen von a_x und c_x. Da aber $f(x)$ nicht durch a_x und c_x theilbar ist, so muss $\Psi(x)$ eine ganze Function sein, und (16) ergiebt, wenn wir mit $\Theta(x)$ eine neue Form von x (vom Grade 16) bezeichnen:

$$(18) \qquad \frac{D(x, a) - f(x)\, \Theta(x)}{a_x^6} = \chi(x).$$

Diese Gleichung zeigt aber, dass die Curve 14ten Grades:

(19) $$\chi(x) = 0,$$

die von den a gänzlich unabhängig ist, durch die Berührungspunkte der Doppeltangenten, aber durch keinen anderen Punkt der Curve $f(x)$ hindurchgeht.

Die Function $\chi(x)$ ist rational von den Coëfficienten der Gleichung $f(x)$ abhängig. Es giebt unendlich viele verschiedene solcher Curven, unter denen sich auch Covarianten von $f(x)$ finden. Man kann sie, wie Hesse nachgewiesen hat, in einfacher Weise durch Determinanten ausdrücken.

Hier ziehen wir daraus den Schluss:

2. Eine Curve vierter Ordnung ohne singulären Punkt hat 28 Doppeltangenten.

Einem Bedenken gegen diesen Schluss ist aber noch zu begegnen. Es wäre denkbar, dass die Curve χ die Curve f berührt, oder dass die Curve f durch singuläre Punkte der Curve χ hindurchgeht. Dann würde sich die Anzahl der Schnittpunkte und möglicherweise auch die Anzahl der Doppeltangenten vermindern, so dass unsere Schlussweise eigentlich nur lehrt, dass eine Curve vierter Ordnung nicht mehr als 28 Doppeltangenten haben kann. Dies Bedenken wird sich aber durch die folgenden Betrachtungen von selbst dadurch erledigen, dass wir Formen der Curvengleichung kennen lernen werden, bei denen die Existenz von 28 verschiedenen Doppeltangenten ersichtlich ist.

§. 96.

Die Steiner'schen Complexe.

Wenn $x_1 = 0$ die Gleichung irgend einer Doppeltangente der Curve vierter Ordnung $f = 0$ ist, die wir kurz die Doppeltangente x_1 nennen, so muss, wenn man $x_1 = 0$ setzt, f in ein Quadrat übergehen. Daraus ergiebt sich, dass f von der Form sein muss:

(1) $$f = x_1 V - u^2,$$

worin V eine cubische, u eine quadratische Form ist. Der Function f kann aber auf dreifach unendlich viele Arten die Gestalt (1) gegeben werden. Denn bedeutet p eine beliebige

lineare Function, die drei willkürliche Constanten enthält, so folgt aus (1):

$$f = x_1 (V + 2pu + x_1 p^2) - (u + p x_1)^2,$$

was wieder von der Form (1) ist.

Ist nun $y_1 = 0$ die Gleichung einer zweiten von x_1 verschiedenen Doppeltangente, so können wir die Constanten in p (und zwar noch auf unendlich viele verschiedene Arten) so wählen, dass der Kegelschnitt $u + p x_1 = 0$ durch die beiden Berührungspunkte von y_1 geht, und wir können daher annehmen, dass schon in der Form (1) die Function u so gewählt sei. Dann muss in denselben Punkten auch die cubische Form V verschwinden.

Aber noch mehr: Da die Linie $y_1 = 0$ Doppeltangente sein soll, so muss, wenn wir x_1, y_1 und irgend eine dritte davon unabhängige lineare Function z als Variable einführen, in den Berührungspunkten

$$f'(x_1) = 0, \quad f'(z) = 0$$

sein, und daraus folgt nach (1):

$$V'(x_1) = 0, \quad V'(z) = 0,$$

d. h. die Curve dritter Ordnung $V = 0$ wird von der Linie $y_1 = 0$ in den Berührungspunkten mit f berührt, und dies ist nur möglich, wenn V zerfällt und die Function y_1 als Theiler enthält. Hiernach erhalten wir eine neue Gestalt der Function f:

(2) $$f = x_1 y_1 v - u^2,$$

worin u, v Functionen zweiten Grades sind.

Sind x_1, y_1 irgend beliebige lineare, u, v quadratische Formen von drei Variablen, so stellt die durch (2) bestimmte Function f, gleich Null gesetzt, eine Curve vierter Ordnung dar, von der x_1 und y_1 zwei Doppeltangenten sind.

Sind umgekehrt x_1 und y_1 zwei beliebige Doppeltangenten einer Curve vierter Ordnung $f = 0$, so kann f auf die Form (2) gebracht werden.

Denken wir uns die Coëfficienten von x_1 und y_1 als variabel, und lassen diese Grössen so variiren, dass x_1 und y_1 sich auf der Curve f schneiden, so wird ein Doppelpunkt eintreten.

Die Doppeltangenten arten aus in zwei von dem Doppelpunkte auslaufende Tangenten.

Fallen die Doppeltangenten in eine Linie zusammen, so treten zwei Doppelpunkte auf.

Dagegen können sehr wohl, ohne dass singuläre Punkte entstehen, die beiden Berührungspunkte einer Doppeltangente zusammenfallen, und so die Doppeltangente in eine vierpunktig berührende Tangente übergehen. Dies tritt ein, wenn die Linie x_1 den Kegelschnitt u berührt.

Auch die Form (2) ist noch mit Beibehaltung von x_1, y_1 auf unendlich viele Arten herzustellen.

Nehmen wir, um dies einzusehen, an, es sei

$$f = x_1 y_1 v - u^2 = x_1 y_1 v_1 - u_1^2,$$

so folgt die identische Gleichung:

$$(3) \qquad x_1 y_1 (v - v_1) = (u - u_1)(u + u_1).$$

Wenn nun $u - u_1$ durch x_1, $u + u_1$ durch y_1 theilbar wäre, so würde im Schnittpunkte von x_1 und y_1 auch u und folglich f verschwinden. Dieser Schnittpunkt würde auf der Curve f liegen, was, so lange die Curve keinen singulären Punkt hat, nicht möglich ist. Es muss also einer der beiden Factoren $u - u_1$, $u + u_1$ in (3) durch $x_1 y_1$ theilbar sein. Da das Vorzeichen von u_1 noch nicht bestimmt ist, so können wir annehmen, es sei $u - u_1$ durch $x_1 y_1$ theilbar, und also bis auf einen constanten Factor mit $x_1 y_1$ identisch. Es wird dann, wenn λ ein solcher Factor ist,

$$u_1 = u + \lambda x_1 y_1,$$

und die Function f erhält die Form:

$$(4) \qquad f = x_1 y_1 (v + 2\lambda u + \lambda^2 x_1 y_1) - (u + \lambda x_1 y_1)^2.$$

Umgekehrt sind für jedes beliebige λ die Formeln (2) und (4) mit einander identisch.

Wenn wir nun λ so bestimmen können, dass die quadratische Function $v + 2\lambda u + \lambda^2 x_1 y_1$ in zwei lineare Factoren zerfällt, so erhält, wenn wir $u + \lambda x_1 y_1 = u_1$ setzen, f nach (4) die Gestalt

$$(5) \qquad f = x_1 y_1 x_2 y_2 - u_1^2,$$

und diese Form zeigt, dass x_2, y_2 **zwei weitere Doppeltangenten sind**, und dass die acht Berührungspunkte der Doppeltangenten x_1, y_1, x_2, y_2 auf einem Kegelschnitte $u_1 = 0$ liegen.

Nun ist die nothwendige und hinreichende Bedingung dafür, dass eine ternäre quadratische Form in zwei lineare Factoren zerfalle, die, dass die Determinante der quadratischen Form verschwinde (Bd. I, §. 56).

Drücken wir die Formen u, v durch x_1, y_1 und irgend eine dritte Variable y aus, und bezeichnen die Coëfficienten in v und u mit a_{ik}, b_{ik}, so dass $2a_{33}$, $2b_{33}$ die Coëfficienten von $x_1 y_1$ werden, so erhalten wir die Bedingung für das Zerfallen von $v + 2\lambda u + \lambda^2 x_1 y_1$ in der Form:

$$(6) \quad \begin{vmatrix} a_{11}+2\lambda b_{11}, & a_{12}+2\lambda b_{12}, & a_{13}+2\lambda b_{13} \\ a_{21}+2\lambda b_{21}, & a_{22}+2\lambda b_{22}, & a_{23}+2\lambda b_{23}+\frac{1}{2}\lambda^2 \\ a_{31}+2\lambda b_{31}, & a_{32}+2\lambda b_{32}+\frac{1}{2}\lambda^2, & a_{33}+2\lambda b_{33} \end{vmatrix} = 0,$$

und dies ist eine Gleichung 5ten Grades in Bezug auf λ, die uns also fünf Zerlegungen giebt:

$$x_2 y_2,\ x_3 y_3,\ x_4 y_4,\ x_5 y_5,\ x_6 y_6.$$

Ueber die Coëfficienten in f lässt sich, wie (6) zeigt, so verfügen, dass alle die so bestimmten Functionen $x_i y_i$ von einander verschieden sind, und daraus folgt, wie oben gezeigt, dass sie verschieden bleiben, so lange die Curve f keine singulären Punkte hat. Es gilt also der folgende Satz:

1. Zu jedem Paare von Doppeltangenten $x_1 y_1$ gehören fünf weitere Paare $x_i y_i$ von der Art, dass die acht Berührungspunkte von $x_1 y_1$ $x_i y_i$ auf einem Kegelschnitte liegen.

Die sechs Paare von Doppeltangenten, die auf diese Weise bestimmt sind:

$$x_1 y_1,\ x_2 y_2,\ x_3 y_3,\ x_4 y_4,\ x_5 y_5,\ x_6 y_6,$$

wollen wir einen Steiner'schen Complex nennen[1]).

Betrachten wir die Paare $x_1 y_1$, $x_2 y_2$, $x_3 y_3$ eines solchen Complexes, und setzen

$$f = x_1 y_1\, x_2 y_2 - u_1^2 = x_1 y_1\, x_3 y_3 - u_2^2,$$

---

[1]) Es ist dafür bisher gewöhnlich der Ausdruck Steiner'sche Gruppe gebraucht. Da aber das Wort „Gruppe" in der Algebra eine ganz bestimmte andere Bedeutung hat, so ziehen wir es vor, diesen Ausdruck hier zu vermeiden.

so folgt daraus die Identität

$$x_1 y_1 (x_2 y_2 - x_3 y_3) = (u_1 - u_2)(u_1 + u_2),$$

und daraus wie oben

$$u_1 - u_2 = h\, x_1 y_1$$
$$u_1 + u_2 = \frac{x_2 y_2 - x_3 y_3}{h},$$

worin h eine Constante bedeutet, also

$$2 u_1 = h\, x_1 y_1 + \frac{x_2 y_2 - x_3 y_3}{h},$$

und danach wird

$$(7) \qquad 4f = 4\, x_1 y_1\, x_2 y_2 - \left(h\, x_1 y_1 + \frac{x_2 y_2 - x_3 y_3}{h}\right)^2.$$

Dieser Gleichungsform können wir eine elegantere Gestalt geben, wenn wir

$$h\, x_1, \quad \frac{x_2}{h}, \quad \frac{x_3}{h}$$

durch

$$x_1, \quad x_2, \quad x_3$$

ersetzen. Dann bedeuten die neuen x_1, x_2, x_3, gleich Null gesetzt, dieselben Linien wie die ursprünglichen, da sich ja beide nur durch einen constanten Factor unterscheiden, und es ergiebt sich aus (7):

$$(8) \qquad \begin{aligned} -4f &= (x_1 y_1 + x_2 y_2 - x_3 y_3)^2 - 4\, x_1 y_1\, x_2 y_2 \\ &= x_1^2 y_1^2 + x_2^2 y_2^2 + x_3^2 y_3^2 \\ &\quad - 2\, x_2 y_2\, x_3 y_3 - 2\, x_1 y_1\, x_2 y_2 - 2\, x_1 y_1\, x_3 y_3, \end{aligned}$$

und die Gleichung $f = 0$ kann auch in der eleganten irrationalen Form

$$x_1 y_1 + x_2 y_2 - x_3 y_3 = -2\sqrt{x_1 y_1\, x_2 y_2}$$

oder

$$(9) \qquad \sqrt{x_1 y_1} + \sqrt{x_2 y_2} + \sqrt{x_3 y_3} = 0$$

dargestellt werden. Aus (9) können wir wieder rückwärts die Form (8) herleiten. Weil aber (9) ganz symmetrisch ist, so können wir die drei Paare vertauschen und erhalten z. B. auch

$$4\, x_2 y_2\, x_3 y_3 = (-x_1 y_1 + x_2 y_2 + x_3 y_3)^2,$$

woraus zu ersehen ist, dass auch die Berührungspunkte von $x_2 y_2\, x_3 y_3$ auf einem Kegelschnitte liegen, und dass in dem Complex, den man aus $x_2 y_2$ erhält, nicht nur das Paar $x_1 y_1$, son-

dern auch das Paar $x_3\, y_3$ und folglich alle Paare $x_i\, y_i$ vorkommen, dass also dieser Complex von dem aus $x_1\, y_1$ abgeleiteten überhaupt nicht verschieden ist. Wir haben also den Satz:

2. Die Paare eines Steiner'schen Complexes haben die Eigenschaft, dass die acht Berührungspunkte von irgend zweien dieser Paare auf einem Kegelschnitte liegen, und dass man immer denselben Complex erhält, von welchem der sechs Paare man ausgehen mag.

Hieraus ergiebt sich, dass drei Doppeltangenten eines Steiner'schen Complexes, wie x_1, y_1, x_2, von denen zwei ein Paar des Complexes bilden, ihre sechs Berührungspunkte auf einem Kegelschnitte haben. Dagegen giebt es wieder Systeme von drei Doppeltangenten (Tripel), deren sechs Berührungspunkte nicht auf einem Kegelschnitte liegen.

Nach einer von Frobenius eingeführten Bezeichnung bilden drei Doppeltangenten, wie x_1, y_1, x_2, deren Berührungspunkte auf einem Kegelschnitte liegen, ein syzygetisches Tripel. Drei Doppeltangenten, deren sechs Berührungspunkte nicht auf einem Kegelschnitte liegen, bilden ein azygetisches Tripel. Entsprechend wollen wir vier Doppeltangenten, deren acht Berührungspunkte auf einem Kegelschnitte liegen, ein syzygetisches Quadrupel, und irgend ein System von Doppeltangenten, von denen je drei azygetisch sind, ein azygetisches System nennen.

Hier gilt nun der folgende wichtige Satz:

3. Drei Doppeltangenten, die in einem Steiner'schen Complexe vorkommen, so dass keine zwei von ihnen ein Paar bilden, wie x_1, x_2, x_3, sind immer azygetisch.

Der Beweis dieses Satzes ergiebt sich einfach aus der Gleichungsform (9). Aus ihr ersieht man zunächst, dass die drei Linien x_1, x_2, x_3 sich nicht in einem Punkte schneiden; denn ein solcher Schnittpunkt würde auf der Curve f liegen und wäre daher ein singulärer Punkt. Wir können also x_1, x_2, x_3 als Coordinaten einführen und demnach

$$\begin{aligned} y_1 &= \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 \\ y_2 &= \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 \\ y_3 &= \gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3 \end{aligned}$$

setzen. Hierin kann keine der drei Constanten α_1, β_2, γ_3 verschwinden. Denn wenn z. B. $\alpha_1 = 0$ ist, so schneiden sich nach (9) die Linien x_2, x_3, y_1 auf der Curve f, und dieser Schnittpunkt müsste ein singulärer Punkt sein.

Nach der Gleichung (9) ergeben sich aber die Coordinaten der Berührungspunkte von x_1, x_2, x_3 aus den folgenden drei Paaren von Gleichungen, von denen jedes Paar zwei Berührungspunkte giebt:

$$\begin{aligned} x_1 &= 0, \quad x_2(\beta_2 x_2 + \beta_3 x_3) - x_3(\gamma_2 x_2 + \gamma_3 x_3) = 0 \\ x_2 &= 0, \quad x_3(\gamma_3 x_3 + \gamma_1 x_1) - x_1(\alpha_3 x_3 + \alpha_1 x_1) = 0 \\ x_3 &= 0, \quad x_1(\alpha_1 x_1 + \alpha_2 x_2) - x_2(\beta_1 x_1 + \beta_2 x_2) = 0. \end{aligned}$$

Sollen nun diese sechs Punkte auf einem Kegelschnitte $\varphi = 0$ liegen, so muss φ, von einem constanten Factor h abgesehen, für $x_1 = 0$ in den linken Theil der zweiten Gleichung des ersten Paares $x_2(\beta_2 x_2 + \beta_3 x_3) - x_3(\gamma_2 x_2 + \gamma_3 x_3)$ übergehen. Bezeichnen wir also mit a_1, a_2, a_3 die Coëfficienten von x_1^2, x_2^2, x_3^2 in φ, so muss

$$\begin{aligned} a_2 &= h_1 \beta_2, \quad a_3 = - h_1 \gamma_3 \\ a_3 &= h_2 \gamma_3, \quad a_1 = - h_2 \alpha_1 \qquad (10) \\ a_1 &= h_3 \alpha_1, \quad a_2 = - h_3 \beta_2 \end{aligned}$$

sein, und hierin sind h_1, h_2, h_3 drei Constanten.

Aus (10) folgt aber:

$$h_2 = - h_3, \quad h_3 = - h_1, \quad h_1 = - h_2,$$

und dies wäre nur möglich, wenn $h_1 = h_2 = h_3 = 0$ wäre.

Dies ist aber nur dann der Fall, wenn a_1, a_2, a_3 verschwinden, wenn also der Kegelschnitt φ durch die Schnittpunkte der drei Geraden x_1, x_2, x_3 geht. Er soll aber durch die Berührungspunkte dieser drei Doppeltangenten gehen, die sicher von ihren drei Schnittpunkten verschieden sind. Also ist unsere Annahme als unmöglich nachgewiesen und der Satz 3. bewiesen.

§. 97.

Complexpaare und Complextripel.

Die Sätze des vorigen Paragraphen geben ein vorzügliches Hülfsmittel, um die mannigfachen geometrischen und algebraischen Beziehungen der Doppeltangenten zu erforschen und dar-

zustellen. Wir beschränken uns hier auf das, was für die Erreichung unseres Hauptzieles, nämlich der Bestimmung der Galois'schen Gruppe des Problems, erforderlich ist.

Wir gehen von einem beliebig herausgegriffenen Steiner'schen Complexe aus:

(1) $$x_1 y_1, \; x_2 y_2, \; x_3 y_3, \; x_4 y_4, \; x_5 y_5, \; x_6 y_6.$$

Die Form der Gleichung §. 96, (5) zeigt dann, dass in dem durch das Paar $x_1 x_2$ bestimmten Complexe das Paar $y_1 y_2$, und in dem durch $x_1 y_2$ bestimmten Complexe das Paar $x_2 y_1$ vorkommen muss.

Wir betrachten also neben (1) die zwei weiteren Complexe:

(2) $$x_1 x_2, \quad y_1 y_2, \quad \ldots$$

(3) $$x_1 y_2, \quad x_2 y_1, \quad \ldots$$

Jeder der beiden Complexe (2), (3) enthält ausser den schon bekannten noch acht weitere Doppeltangenten, und diese müssen alle von den x_i, y_i verschieden sein, weil, wenn z. B. x_3 in (2) vorkäme, $x_1 x_2 x_3$ syzygetisch wäre, was dem Satze 3., (§. 96) widerspricht. Ebenso können die beiden Complexe (2) und (3) ausser x_1, x_2, y_1, y_2 keine gemeinsame Doppeltangente enthalten. Denn wenn etwa z in beiden vorkäme, so wären $x_1 x_2 z$ nach (2) syzygetisch, nach (3) azygetisch, was ein Widerspruch ist. Daraus folgt:

4. In den drei Complexen (1), (2), (3) zusammengenommen kommen alle 28 Doppeltangenten vor.

Hieraus folgt, dass jede Doppeltangente, die mit irgend einem Paare $x_1 y_1$ ein syzygetisches Tripel bildet, in dem Complexe $x_1 y_1$ vorkommen muss, dass also jedes syzygetische Tripel durch eine bestimmte weitere Doppeltangente zu einem syzygetischen Quadrupel ergänzt wird, und dass folglich ein Kegelschnitt, der durch die Berührungspunkte von drei Doppeltangenten hindurchgeht, die Curve f in den Berührungspunkten einer vierten Doppeltangente schneidet.

Zwei Paare eines Complexes bilden immer ein syzygetisches Quadrupel, und wie man ein solches Quadrupel auch in zwei Paare theilen mag, beide Paare gehören immer demselben Complexe an.

Da man aus 28 Dingen 14.27 Paare bilden kann, da jedes Paar von Doppeltangenten einen Complex bestimmt und in jedem

Complexe sechs Paare vorkommen, so ist die Gesammtzahl der Complexe $14.27:6 = 63$.

5. Es giebt 63 Steiner'sche Complexe.

Wenn wir aus den Paaren des Complexes (1) statt $x_1 y_1$, $x_2 y_2$ irgend ein anderes Paar von Paaren herausgreifen, so können wir daraus nach dem Schema von (2) und (3) jedesmal zwei neue Complexe bilden. Da es 15 solcher Paare von Paaren giebt, so erhalten wir 30 neue Complexe vom Typus (2), (3), die alle in gleicher Weise aus dem Complexe (1) abgeleitet sind, und die alle unter einander verschieden sind.

Nehmen wir nun irgend eine von den in (2) und (3) neu hinzutretenden Doppeltangenten z_1, so erhalten wir zwei neue Complexe, wenn wir von den beiden Paaren $x_1 z_1$, $y_1 z_1$ ausgehen, und da wir z_1 auf 16 verschiedene Arten wählen können, so ergeben sich so 32 neue Complexe, womit die Gesammtzahl aller Complexe erschöpft ist. Es muss aber noch die Vertheilung der Doppeltangenten auf die Complexe $x_1 z_1$, $y_1 z_1$ genauer untersucht werden.

Wir können, ohne die Allgemeinheit zu beschränken, da wir nöthigenfalls x_1 mit y_1 vertauschen können, die Annahme machen, dass z_1 in dem Complexe (2) und darin in dem Paare $z_1 z_2$ vorkomme.

Dann erhalten wir die beiden Complexe:

$$\begin{array}{ll} (4) & x_1 z_1,\ x_2 z_2,\ \dots \\ (5) & y_1 z_1,\ y_2 z_2,\ \dots \end{array}$$

Wir betrachten jetzt die drei Complexe:

$$\begin{array}{ll} (4) & x_1 z_1,\ x_2 z_2,\ \dots \\ (2) & x_1 x_2,\ z_1 z_2,\ \dots \\ (4\,\text{a}) & x_1 z_2,\ x_2 z_1,\ \dots, \end{array}$$

die nach dem Satze 4. alle Doppeltangenten enthalten müssen, darunter also auch x_3, y_3. Diese kommen aber nicht in (2) vor, und ebenso können nicht beide in (4) oder beide in (4 a) vorkommen, da sonst x_1, x_3, y_3 azygetisch sein müssten, während sie doch [nach (1)] syzygetisch sind. Da wir eventuell x_3 und y_3 in der Bezeichnung vertauschen dürfen, so können wir annehmen, dass x_3 in (4) vorkomme, und zwar in einem Paare $x_3 z_3$.

Dann kann, da $z_1 z_2 z_3$ azygetisch sind, z_3 nicht in dem Complexe (2) vorkommen und muss folglich in (3) enthalten sein.

Nun haben wir die beiden Complexe:

$$(4)\qquad x_2 z_2,\ x_3 z_3,\ \ldots$$
$$(4\,b)\qquad x_2 x_3,\ z_2 z_3,\ \ldots,$$

und da $x_2 x_3\ y_2 y_3$ ein syzygetisches Quadrupel sind, so enthält die Gruppe (4 b) auch das Paar $y_2 y_3$, und folglich sind auch $y_2 y_3\ z_2 z_3$ ein syzygetisches Quadrupel. Daraus folgt weiter, dass $y_2 z_2$ und $y_3 z_3$ in denselben Complex gehören. Da man dieselbe Betrachtung wie für $x_3 y_3$ auch für die Paare $x_4 y_4$, $x_5 y_5$, $x_6 y_6$ durchführen kann, so lassen sich hiernach die Complexe (4), (5) vollständig bilden, und sie erhalten den Ausdruck:

$$(4)\qquad x_1 z_1,\ x_2 z_2,\ x_3 z_3,\ x_4 z_4,\ x_5 z_5,\ x_6 z_6$$
$$(5)\qquad y_1 z_1,\ y_2 z_2,\ y_3 z_3,\ y_4 z_4,\ y_5 z_5,\ y_6 z_6.$$

Hierin bilden $z_1 z_2$ ein Paar des Complexes (2) und z_3, z_4, z_5, z_6, die ein azygetisches System bilden, kommen alle in dem Complex (3) vor, in dem keine zwei gepaart sind.

Da wir, wie vorhin gezeigt, nach dem Typus (2), (3), (4), (5) aus dem willkürlich angenommenen Complex (1) alle überhaupt existirenden Complexe ableiten können, so ergiebt sich der Satz:

6. Irgend zwei Complexe haben entweder ein syzygetisches Quadrupel oder ein azygetisches System von sechs Doppeltangenten gemein.

Zwei Complexe, die ein syzygetisches Quadrupel gemein haben, wollen wir ein syzygetisches Complexpaar nennen. Zu jedem solchen Paare giebt es einen dritten Complex, der dasselbe Quadrupel enthält. Drei solche Complexe nennen wir ein syzygetisches Complextripel [z. B. (1), (2), (3)].

Ebenso nennen wir zwei Complexe der zweiten Art, d. h. solche, die sechs azygetische Elemente gemein haben, ein azygetisches Complexpaar.

Jedes azygetische Complexpaar wird gleichfalls durch einen bestimmten Complex, der mit jedem der beiden Complexe ein azygetisches Paar bildet, zu einem Tripel ergänzt [wie (1), (4), (5)]. Ein solches nennen wir ein azygetisches Complextripel.

In einem syzygetischen Tripel kommen alle 28 Doppeltangenten vor, in einem azygetischen nur 18.

§. 98.

Die Aronhold'schen Siebener-Systeme.

Von besonderer Wichtigkeit sind die azygetischen Systeme von sieben Doppeltangenten, die zuerst von Aronhold betrachtet sind, und die daher Aronhold'sche Siebener-Systeme heissen. Wir nennen sie auch vollständige Siebener-Systeme oder kurz vollständige Systeme.

Dass es solche Systeme giebt, zeigen die Zusammenstellungen des vorigen Paragraphen. Denn wenn

$$(1) \qquad \begin{array}{l} x_1 y_1,\ x_2 y_2,\ x_3 y_3,\ x_4 y_4,\ x_5 y_5,\ x_6 y_6 \\ x_1 z_1,\ x_2 z_2,\ x_3 z_3,\ x_4 z_4,\ x_5 z_5,\ x_6 z_6 \end{array}$$

ein azygetisches Complexpaar ist, so ist

$$x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ y_6,\ z_6$$

ein vollständiges Siebener-System (weil in dem Complexe $y_6 z_6$ keines der x vorkommt). Es wird sich zeigen, dass keine azygetischen Systeme von mehr als sieben Elementen bestehen. Es gilt zunächst der Satz:

7. Irgend sechs Elemente eines vollständigen Systemes kommen in einem und nur in einem Complexe vor.

Wir beweisen zunächst den zweiten Theil der Behauptung, d. h. wir beweisen, dass, wenn

$$(2) \qquad x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ x_6,\ x_7$$

ein vollständiges System ist, x_1, x_2, x_3, x_4, x_5, x_6 nicht in zwei verschiedenen Complexen vorkommen können. Nehmen wir an, es sei dies möglich, so müssen die beiden Complexe ein azygetisches Paar wie (1) bilden. In dem syzygetischen Tripel

$$\begin{array}{l} y_1 z_1,\ y_2 z_2,\ y_3 z_3,\ y_4 z_4,\ y_5 z_5,\ y_6 z_6 \\ y_1 y_2,\ z_1 z_2,\ x_1 x_2 \\ y_1 z_2,\ y_2 z_1 \end{array}$$

müssen die Doppeltangenten x_3, x_4, x_5, x_6, x_7 vorkommen, und da sie weder im ersten noch im zweiten dieser Complexe vorkommen, so müssen sie im dritten vorkommen. Da in diesem Complexe aber nur noch vier Paare übrig sind, so müssen minde-

stens zwei von den $x_3, \ldots x_7$ ein Paar darin bilden. Das ist aber nicht möglich, da dieses Paar sonst mit einem der übrigen x ein syzygetisches Tripel bilden würde.

Um nachzuweisen, dass die Doppeltangenten $x_1, x_2, x_3, x_4, x_5, x_6$ immer in einem Complexe vorkommen, nehmen wir zwei beliebige von ihnen, $x_1\, x_2$, heraus und wählen ein in dem Complexe $x_1\, x_2$ vorkommendes anderes Paar $y_1\, y_2$, was auf fünf Arten möglich ist. Daraus bilden wir das syzygetische Complextripel

$$(2) \qquad \begin{array}{ll} \alpha) & x_1 x_2,\ y_1 y_2 \\ \beta) & x_1 y_1,\ x_2 y_2 \\ \gamma) & x_1 y_2,\ x_2 y_1, \end{array}$$

welches fünf verschiedene solcher Tripel repräsentirt. In β) und γ) müssen nun x_3, x_4, x_5, x_6, x_7 vorkommen, und zwar keine zwei von ihnen gepaart. Wir zeigen nun zunächst, dass sich diese fünf x nicht zu zwei und drei auf die beiden Complexe β), γ) vertheilen können, sondern nur zu eins und vier. Nehmen wir nämlich an, die Complexe β), γ) seien so zusammengesetzt:

$$(2) \qquad \begin{array}{ll} \beta) & x_1 y_1,\ x_2 y_2,\ x_3 y_3,\ x_4 y_4,\ x_5 y_5,\ . \\ \gamma) & x_1 y_2,\ x_2 y_1,\ x_6 y_6,\ x_7 y_7,\ .\quad ., \end{array}$$

so können wir noch den Complex

$$(2) \qquad \delta) \quad x_6 x_7,\ y_6 y_7 \ldots,$$

betrachten, der mit β) zusammen ein syzygetisches Paar bildet, weil weder x_1 noch y_1 in δ) vorkommt, das Paar also nicht azygetisch sein kann. Es müssen also β) und δ) ein syzygetisches Quadrupel gemein haben, und da in zwei Paaren von β) mindestens ein von x_6, x_7 verschiedenes x vorkommt, so muss dieses x auch in δ) vorkommen, was unmöglich ist, weil kein x mit x_6, x_7 syzygetisch ist. Es bleibt also für β), γ) nur eine Zusammensetzung übrig, wie die folgende:

$$(3) \qquad \begin{array}{ll} \beta) & x_1 y_1,\ x_2 y_2,\ x_3 y_3,\ x_4 y_4,\ x_5 y_5,\ x_6 y_6 \\ \gamma) & x_1 y_2,\ x_2 y_1,\ x_7 y_7,\ .\quad .\quad . \end{array}$$

Dass wir gerade diese Annahme machen, und nicht die sechs x in γ) aufnehmen, ist keine Beschränkung, da wir, wenn nöthig, y_1 mit y_2 vertauschen können.

Wenn wir nun unter Festhaltung von $x_1\, x_2$ an Stelle von $y_1\, y_2$ die anderen Paare von (2) α) treten lassen, so bekommen

wir fünf Complexbildungen vom Typus (3). Zwei solche Complexbildungen können sich aber nur dadurch unterscheiden, dass an Stelle von x_7 jedesmal ein anderes der Elemente x_3, x_4, x_5, x_6, x_7 tritt, und alle diese Möglichkeiten müssen auch vorkommen, weil wir sonst zwei verschiedene Complexe erhalten würden, die dieselben sechs Elemente des vollständigen Systems der x enthalten, was nicht möglich ist, wie wir bewiesen haben. Demnach können wir annehmen, dass die in dem Complexe (3) β) vorkommenden $x_1, x_2, x_3, x_4, x_5, x_6$ irgend welche sechs Elemente des vollständigen Systemes seien, was bewiesen werden sollte.

§. 99.

Der Hesse-Cayley'sche Algorithmus zur Bezeichnung der Doppeltangenten.

Der Satz 7. des vorigen Paragraphen führt zu einer Bezeichnungsweise für die Doppeltangenten, durch die eine sehr übersichtliche Darstellung aller dieser Verhältnisse möglich ist, die von Cayley (im Anschluss an Hesse) ausgebildet ist.

Wir legen ein vollständiges Siebener-System

$$x_1, x_2, x_3, x_4, x_5, x_6, x_7$$

zu Grunde, dessen Elemente wir einfach durch die Ziffern 1, 2, 3, 4, 5, 6, 7 bezeichnen. Wir sondern eine beliebige Doppeltangente, etwa x_1, dieses Systemes aus, und bilden den Complex, der die übrigen sechs enthält:

$$(1) \qquad x_2 y_2, \ x_3 y_3, \ x_4 y_4, \ x_5 y_5, \ x_6 y_6, \ x_7 y_7.$$

Die Doppeltangente y_2 ist dann durch das gewählte x_1 und durch x_2 völlig bestimmt und kann daher durch [1 2] bezeichnet werden. Ebenso bezeichnen wir y_3 durch [1 3] u. s. f. Die Doppeltangenten [1 2], [1 3], ..., [1 7] sind hierdurch vollständig bestimmt und von einander verschieden. Aus dieser Bestimmung geht auch hervor, was man allgemein unter $[\mu\ \nu]$ zu verstehen hat, wenn μ, ν zwei verschiedene Ziffern aus der Reihe 1 bis 7 bedeuten.

Es ist nun zunächst zu zeigen, dass $[\mu\ \nu] = [\nu\ \mu]$ ist. Es genügt, wenn wir nachweisen, dass $[1\ 2] = [2\ 1]$ ist. Dazu brauchen wir nur den Complex zu bilden, der $x_1, x_3, x_4, x_5, x_6, x_7$

enthält, und der mit (1) ein azygetisches Paar bildet. Er muss also von der Gestalt sein:

(2) $$x_1 y_2, \; x_3 z_3, \; x_4 z_4, \; x_5 z_5, \; x_6 z_6, \; x_7 z_7,$$

und demnach ist y_2 auch durch [2 1] zu bezeichnen, w. z. b. w.

Die z in (2) sind von den y in (1) verschieden, und da z. B. $z_3 = [2\ 3]$ ist, so folgt, dass allgemein zwei $[\mu\ \nu]$, die nicht in beiden Ziffern μ, ν übereinstimmen, von einander verschieden sind. Da man aus sieben Ziffern einundzwanzig Paare bilden kann, so erhält man auf diese Weise alle Doppeltangenten und jede nur einmal.

Aus dieser Darstellungsweise ergiebt sich auch, dass keine azygetischen Systeme von mehr als sieben Doppeltangenten existiren; denn fügen wir zu den sieben x noch eine beliebige weitere Doppeltangente, für die wir bei der Gleichberechtigung der Ziffern 1 bis 7 etwa $y_2 = [1\ 2]$ wählen können, so ist $y_2\, x_1\, x_2$ ein syzygetisches Tripel.

Es ist zweckmässig, eine achte Ziffer 8 einzuführen, und die Elemente des ursprünglichen Siebener-Systems nicht durch die einfachen Ziffern, sondern durch die Paare

$$[1\ 8],\ [2\ 8],\ [3\ 8],\ [4\ 8],\ [5\ 8],\ [6\ 8],\ [7\ 8]$$

zu bezeichnen, wobei dann auch gelten soll, dass $[1\ 8] = [8\ 1]$ u. s. f. ist. Dann werden alle 28 Doppeltangenten übereinstimmend durch die Paare $[\mu\ \nu]$ bezeichnet, in denen μ und ν zwei verschiedene Ziffern der Reihe 1 bis 8 bedeuten.

Dabei ist es für die Uebersichtlichkeit sehr förderlich, wenn man eine anschauliche Bezeichnung anwendet [1]). Man deutet eine Doppeltangente $[\mu\ \nu]$ durch einen einfachen Strich | an, an dessen Enden man sich die beiden Ziffern μ, ν gesetzt denkt. Dann bedeuten zwei Striche ohne gemeinsamen Punkt || zwei Doppeltangenten, in deren Bezeichnung $[\mu\ \nu]$ keine gemeinschaftliche Ziffer vorkommt, und zwei von einem Punkte auslaufende Striche, \/, zwei Doppeltangenten, die in ihren Symbolen $[\mu\ \nu]$ eine gemeinschaftliche Ziffer haben. Hiernach sind die complicirteren Zeichen, die wir nachher anwenden, von selbst verständlich. Für ein Tripel von Doppeltangenten haben wir z. B. folgende fünf Zeichen |||, ⊓, △, \|/, \/|.

---

[1]) Nach Cayley; vergl. Salmon, „Higher plane curves“.

Es soll jetzt zunächst untersucht werden, wie sich in dieser Bezeichnungsweise die azygetischen und die syzygetischen Tripel unterscheiden.

Dabei ist zu beachten, dass nach der bis jetzt gegebenen Erklärung die Ziffer 8 eine besondere Stelle einnimmt, während die Ziffern 1 bis 7 vollständig gleichartig auftreten und beliebig permutirt werden können.

Wir leiten aus den beiden Complexen (1), (2) noch die Ergänzung zu einem azygetischen Complextripel her, nämlich:

$$\begin{array}{l} x_2 y_2,\ x_3 y_3,\ x_4 y_4,\ x_5 y_5,\ x_6 y_6,\ x_7 y_7, \\ x_1 y_2,\ x_3 z_3,\ x_4 z_4,\ x_5 z_5,\ x_6 z_6,\ x_7 z_7, \\ x_1 x_2,\ y_3 z_3,\ y_4 z_4,\ y_5 z_5,\ y_6 z_6,\ y_7 z_7, \end{array} \tag{3}$$

und gehen nun die einzelnen Zeichen für die Doppeltangententripel durch.

Wir beginnen mit dem Zeichen \|/, für welches wir mit Rücksicht auf die Ausnahmestellung der Ziffer 8 drei Typen zu betrachten haben:

$$\begin{array}{l} [1\,8]\ [2\,8]\ [3\,8] = x_1 x_2 x_3 \\ [1\,5]\ [1\,6]\ [1\,7] = y_5 y_6 y_7 \\ [1\,6]\ [1\,7]\ [1\,8] = y_6 y_7 x_1, \end{array} \tag{4}$$

und der Anblick der drei Complexe (3) zeigt (nach dem Satze §. 96, 3.), dass alle diese Tripel azygetisch sind.

Zweitens betrachten wir das Zeichen \/|, für welches vier Typen zu berücksichtigen sind:

$$\begin{array}{l} [8\,3]\ [8\,4]\ [1\,2] = x_3 x_4 y_2 \\ [8\,4]\ [1\,4]\ [2\,3] = x_4 y_4 z_3 \\ [1\,2]\ [1\,3]\ [4\,8] = y_2 y_3 x_4 \\ [1\,4]\ [1\,5]\ [2\,3] = y_4 y_5 z_3, \end{array} \tag{5}$$

und auch diese Tripel sind azygetisch.

Für das Zeichen △ ist zu betrachten:

$$\begin{array}{l} [1\,8]\ [2\,8]\ [1\,2] = x_1 x_2 y_2 \\ [1\,2]\ [1\,3]\ [2\,3] = y_2 y_3 z_3, \end{array} \tag{6}$$

die sich gleichfalls als azygetisch erweisen, weil y_2 in dem Complexe (3), der die Paare $x_1 x_2$, $y_3 z_3$ enthält, nicht vorkommt.

Für das Zeichen ||| giebt es zwei Typen:

$$\begin{array}{l} [1\,3]\ [2\,4]\ [5\,8] = y_3 z_4 x_5 \\ [1\,3]\ [2\,4]\ [5\,6] = y_3 z_4 [5\,6]. \end{array} \tag{7}$$

Betrachten wir das syzygetische Complextripel

$$(8)\qquad \begin{array}{llll} y_3 z_4, & y_4 z_3, & \ldots\ldots & \\ y_3 y_4, & z_3 z_4, & x_3 x_4 & \ldots \\ y_3 z_3, & y_4 z_4, & \ldots\ldots, & \end{array}$$

in dem alle Doppeltangenten vorkommen müssen, so finden wir [5 8] und [5 6] nicht in den beiden letzten Complexen von (8), weil

$$(9)\qquad \begin{array}{ll} y_3 z_3 [5\,8] = [1\,3]\,[2\,3]\,[5\,8], & y_3 y_4 [5\,8] = [1\,3]\,[1\,4]\,[5\,8] \\ y_3 z_3 [5\,6] = [1\,3]\,[2\,3]\,[5\,6], & y_3 y_4 [5\,6] = [1\,3]\,[1\,4]\,[5\,6] \end{array}$$

das Zeichen $\vee|$ haben und daher azygetisch sind. Folglich kommen [5 8] und [5 6] im ersten der Complexe (8) vor, und die beiden Tripel (7) sind syzygetisch.

Endlich haben wir auch das Zeichen $\sqcap$ zu betrachten, das wieder drei Typen giebt:

$$(10)\qquad \begin{array}{l} [1\,2]\,[2\,3]\,[3\,4] = y_2 z_3 [3\,4] \\ [1\,2]\,[2\,3]\,[3\,8] = y_2 z_3 x_3 \\ [1\,8]\,[8\,2]\,[2\,3] = x_1 x_2 z_3. \end{array}$$

Auch diese Tripel sind syzygetisch, was für die beiden letzten unmittelbar aus dem Complextripel (3) zu ersehen ist, und für das erste aus dem syzygetischen Complextripel

$$\begin{array}{lll} y_2 z_3, & x_1 x_3, & \ldots\ldots \\ y_2 x_1, & z_3 x_3, & \ldots\ldots \\ y_2 x_3, & z_3 x_1, & \ldots\ldots, \end{array}$$

folgt, von denen die beiden letzten [3 4] nicht enthalten, weil $y_2 x_1 [3\,4]$ und $y_2 x_3 [3\,4]$ beide das Zeichen $\vee|$ haben.

Hier ist aber die Ausnahmestellung der Ziffer 8 gänzlich verschwunden, und wir kommen zu dem Resultate:

Unter den Tripeln von Doppeltangenten sind die mit den Zeichen

$$|||,\ \sqcap$$

syzygetisch, und die mit den Zeichen

$$\vee|,\ \triangle,\ \vee|$$

azygetisch.

Hieraus erhält man sehr leicht die Zeichen für sämmtliche syzygetische und azygetische Quadrupel:

Die Quadrupel von Doppeltangenten mit den Zeichen

||||, □

sind syzygetisch, und die mit den Zeichen

\|/, Δ|, \/|, \/\/

azygetisch.

Alle übrigen Quadrupel sind weder syzygetisch noch azygetisch.

Hiernach ist es leicht, die Zeichen für sämmtliche vollständige Siebener-Systeme zu bilden.

Ein solches Zeichen muss aus sieben Strichen bestehen, die nicht mehr als acht Eckpunkte haben können und die eine Figur bilden, aus der sich keine der beiden Figuren |||, ⊓ ablösen lässt. Daraus folgt zunächst, dass diese Figur aus nicht mehr als zwei getrennten Theilen bestehen kann, weil sonst die Figur ||| darin enthalten wäre, und dass kein Theil mehr als ein Centrum haben kann, von dem mehrere Striche auslaufen, ausser wenn dieser Theil das Dreieck Δ ist, weil sonst die Figur ⊓ vorkommen würde.

Wenn nun die Figur eintheilig ist, so muss sie ein siebenstrahliger Stern ✳ sein, und da man jede der acht Ziffern als Mittelpunkt wählen kann, so sind dies acht Möglichkeiten, von denen eine die oben betrachtete Annahme ist:

[18] [28] [38] [48] [58] [68] [78].

Ist aber die Figur zweitheilig, so ist zunächst auszuschliessen, dass der eine Theil aus einem oder aus zwei Strichen oder einem dreistrahligen Sterne besteht; denn in diesen Fällen müsste der andere Theil ein Stern mit sechs, fünf oder vier Strahlen sein. Dazu aber bleiben von den acht Ziffern nicht mehr genug übrig. Es bleibt also nur noch übrig, dass der eine Theil ein Dreieck, der andere ein vierstrahliger Stern ist, Δ \|/, und diese Annahme ist auch in der That immer zulässig. Ein Repräsentant eines solchen Systems ist:

[12] [13] [23] [45] [46] [47] [48].

Das Dreieck kann man auf $8.7.6 : 2.3 = 56$ verschiedene Arten wählen, und zu jedem Dreieck giebt es noch fünf Möglichkeiten, den vierstrahligen Stern anzunehmen, da man jeden der übrigen fünf Punkte zum Centrum machen kann. Die Anzahl

dieser Bestimmungen ist daher 280, und wir kommen zu folgendem Resultate:

Es giebt im Ganzen 288 Aronhold'sche Systeme, deren Zeichen eine der beiden Gestalten hat

✳; Δ⩛.

Aus diesen Zeichen darf man aber nicht etwa schliessen, dass diese Siebener-Systeme in zwei verschiedene Arten zerfallen. Der Unterschied der beiden Figuren liegt nur in der Bezeichnung. In der That können wir ja von einem ganz beliebigen der vollständigen Siebener-Systeme ausgehen, um die Bezeichnung abzuleiten.

Hiernach findet man leicht die Bezeichnung für die Steiner'schen Complexe, die nach einem der beiden folgenden Typen zu bilden sind:

[1 2] [3 4], [1 3] [2 4], [1 4] [2 3], [5 6] [7 8], [5 7] [6 8], [5 8] [6 7],
[1 7] [1 8], [2 7] [2 8], [3 7] [3 8], [4 7] [4 8], [5 7] [5 8], [6 7] [6 8].

§. 100.

Rationale Bestimmung der Curve aus einem vollständigen Siebener-Systeme.

Die grosse Bedeutung der Aronhold'schen Systeme für das Problem der Doppeltangenten spricht sich in folgenden beiden Sätzen aus:

I. **Ist bei einer Curve vierter Ordnung ein vollständiges Siebener-System gegeben, so können daraus alle übrigen Doppeltangenten rational bestimmt werden.**

II. **Sind sieben beliebige gerade Linien in einer Ebene gegeben, so kann man im Allgemeinen, d. h. wenn gewisse rationale Functionen von den Coëfficienten in den Gleichungen dieser Geraden nicht verschwinden, auf rationalem Wege die Gleichung einer Curve vierter Ordnung ohne singulären Punkt bestimmen, für die die gegebenen sieben Linien ein Aronhold'sches System bilden.**

Um den ersten Satz zu beweisen, würde es bei der vollkommenen Gleichberechtigung der Ziffern 1 bis 7 genügen, die

Bestimmung von einer achten Doppeltangente aus einem gegebenen vollständigen Systeme durchzuführen. Wir bestimmen aber besser gleichzeitig drei. Es sei also jetzt

(1) $$x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ x_6,\ x_7$$

ein als bekannt vorausgesetztes vollständiges Siebener-System. Wir denken uns die drei Steiner'schen Complexe gebildet, in denen je sechs der Doppeltangenten (1), mit Ausschluss zuerst von x_1, dann von x_2, zuletzt von x_3 enthalten sind.

Die darin neu hinzutretenden 15 Doppeltangenten bezeichnen wir mit dem Buchstaben ξ und erhalten diese drei Complexe [nach §. 99, (1), (2)] in der Gestalt:

(2) $$\begin{array}{l} x_2\,\xi_3,\ x_3\,\xi_2,\ x_4\,\xi_{41},\ x_5\,\xi_{51},\ x_6\,\xi_{61},\ x_7\,\xi_{71} \\ x_3\,\xi_1,\ x_1\,\xi_3,\ x_4\,\xi_{42},\ x_5\,\xi_{52},\ x_6\,\xi_{62},\ x_7\,\xi_{72} \\ x_1\,\xi_2,\ x_2\,\xi_1,\ x_4\,\xi_{43},\ x_5\,\xi_{53},\ x_6\,\xi_{63},\ x_7\,\xi_{73}, \end{array}$$

und nach der Bezeichnung des §. 99 ist

$$\xi_1 = [2\,3],\ \xi_2 = [3\,1],\ \xi_3 = [1\,2],\ \xi_{41} = [1\,4], \ldots$$

Aus (2) ergiebt sich noch ein Steiner'scher Complex, der mit jedem der Complexe (2) ein syzygetisches Paar bildet:

(3) $$x_1\,\xi_1,\ x_2\,\xi_2,\ x_3\,\xi_3,\ \ldots$$

und dieser Complex enthält keine der Doppeltangenten x_4, x_5, x_6, x_7.

Indem wir nun die gesuchten Functionen ξ_1, ξ_2, ξ_3 mit den geeigneten constanten Factoren multiplicirt annehmen, können wir die Gleichung der Curve vierter Ordnung nach §. 96, (9) in die Form

(4) $$\sqrt{x_1\,\xi_1} + \sqrt{x_2\,\xi_2} + \sqrt{x_3\,\xi_3} = 0$$

setzen, und also die rationale Function f, die, gleich Null gesetzt, die Gleichung der Curve giebt, in jeder der drei mit einander identischen Formen

(5) $$f = 4\,x_2\,\xi_2\,x_3\,\xi_3 - u_1^2 = 4\,x_3\,\xi_3\,x_1\,\xi_1 - u_2^2 = 4\,x_1\,\xi_1\,x_2\,\xi_2 - u_3^2,$$

annehmen, worin

(6) $$\begin{array}{l} u_1 = -\,x_1\,\xi_1 + x_2\,\xi_2 + x_3\,\xi_3 \\ u_2 = \,x_1\,\xi_1 - x_2\,\xi_2 + x_3\,\xi_3 \\ u_3 = \,x_1\,\xi_1 + x_2\,\xi_2 - x_3\,\xi_3 \end{array}$$

gesetzt ist. Nun bilden [nach (2)] auch $x_2\,\xi_3\,x_4\,\xi_{41}$ ein syzygetisches Quadrupel, und folglich können wir, wenn über einen

constanten Factor in ξ_{41} verfügt wird, f auch in der Form darstellen:

(7) $$f = 4\,x_2\,\xi_3\,x_4\,\xi_{41} - v^2,$$

worin v eine quadratische Form ist. Hieraus und aus der ersten Darstellung in (5) ergiebt sich aber die Identität

$$4\,x_2\,\xi_3\,(x_3\,\xi_2 - x_4\,\xi_{41}) = (u_1 - v)\,(u_1 + v),$$

und daraus schliessen wir, dass einer der beiden Factoren rechts durch $x_2\,\xi_3$ theilbar sein muss [§. 96, (3)]. Nehmen wir an, es sei dies $u_1 - v$, was durch Verfügung über das Vorzeichen von v erreicht werden kann, so folgt, dass ein von Null verschiedener constanter Factor λ existiren muss, so dass

$$u_1 - v = 2\,\lambda_1\,x_2\,\xi_3,$$

$$u_1 + v = \frac{2\,(x_3\,\xi_2 - x_4\,\xi_{41})}{\lambda_1},$$

woraus

$$u_1 = \lambda_1\,x_2\,\xi_3 + \frac{x_3\,\xi_2 - x_4\,\xi_{41}}{\lambda_1}$$

folgt. Ersetzen wir hierin u_1 durch seinen Ausdruck aus (6), so ergiebt sich

$$x_4\,\xi_{41} = x_3\,\xi_2 - \lambda_1\,(-x_1\,\xi_1 + x_2\,\xi_2 + x_3\,\xi_3) + \lambda_1^2\,x_2\,\xi_3.$$

Solcher Gleichungen erhalten wir zunächst drei, wenn wir die Indices 1, 2, 3 cyklisch vertauschen und an Stelle der unbekannten Constanten λ_1 drei Constanten $\lambda_1, \lambda_2, \lambda_3$ setzen:

(8) $$\begin{aligned} x_4\,\xi_{41} &= x_3\,\xi_2 - \lambda_1\,(-x_1\,\xi_1 + x_2\,\xi_2 + x_3\,\xi_3) + \lambda_1^2\,x_2\,\xi_3 \\ x_4\,\xi_{42} &= x_1\,\xi_3 - \lambda_2\,(x_1\,\xi_1 - x_2\,\xi_2 + x_3\,\xi_3) + \lambda_2^2\,x_3\,\xi_1 \\ x_4\,\xi_{43} &= x_2\,\xi_1 - \lambda_3\,(x_1\,\xi_1 + x_2\,\xi_2 - x_3\,\xi_3) + \lambda_3^2\,x_1\,\xi_2. \end{aligned}$$

Um die Constanten $\lambda_1, \lambda_2, \lambda_3$ zu bestimmen, dividiren wir die beiden letzten dieser Gleichungen mit λ_2 und λ_3 und addiren. Dadurch folgt die identische Gleichung

(9) $$x_4\left(\frac{\xi_{42}}{\lambda_2} + \frac{\xi_{43}}{\lambda_3}\right) =$$
$$x_1\left(-2\,\xi_1 + \lambda_3\,\xi_2 + \frac{\xi_3}{\lambda_2}\right) + \xi_1\left(\lambda_2\,x_3 + \frac{x_2}{\lambda_3}\right).$$

Da nun x_4, x_1, ξ_1 azygetisch sind, und folglich nicht durch einen Punkt gehen können, so muss die Linie

$$\lambda_2\,x_3 + \frac{x_2}{\lambda_3} = 0$$

durch den Schnitt von x_1 und x_4 gehen, und folglich ist x_4 aus x_1 und $\lambda_2 x_3 + \frac{x_2}{\lambda_3}$ linear zusammengesetzt. Nun aber können wir x_4 linear durch x_1, x_2, x_3 ausdrücken, etwa in der Form

$$(10) \qquad x_4 = a_1 x_1 + a_2 x_2 + a_3 x_3,$$

und darin sind a_1, a_2, a_3 als bekannt zu betrachten, und keine dieser Constanten kann verschwinden. Es ist also $\lambda_2 \lambda_3 = a_3 : a_2$, und wenn wir eine neue Constante h_1 einführen, so ist

$$(11) \qquad \lambda_2 = h_1 a_3, \quad \frac{1}{\lambda_3} = h_1 a_2,$$

und die Gleichung (9) ergiebt die Identität:

$$h_1 x_4 \left(\frac{\xi_{42}}{\lambda_2} + \frac{\xi_{43}}{\lambda_3} - h_1 \xi_1\right) = x_1 \left(-h_1 (2 + a_1 h_1) \xi_1 + \frac{\xi_2}{a_2} + \frac{\xi_3}{a_3}\right).$$

Daraus schliesst man weiter, wenn k_1 eine neue Constante ist,

$$(12) \qquad \begin{aligned} k_1 x_4 &= - h_1 (2 + a_1 h_1) \xi_1 + \frac{\xi_2}{a_2} + \frac{\xi_3}{a_3}, \\ \frac{\xi_{42}}{\lambda_2} + \frac{\xi_{43}}{\lambda_3} &= h_1 \xi_1 + \frac{k_1}{h_1} x_1. \end{aligned}$$

Wenn man hierin die Ziffern 1, 2, 3 cyklisch vertauscht, so ergeben sich aus (8) drei solche Systeme; zunächst:

$$(13) \qquad \begin{aligned} k_1 x_4 &= - h_1 (2 + a_1 h_1) \xi_1 + \frac{\xi_2}{a_2} + \frac{\xi_3}{a_3} \\ k_2 x_4 &= \frac{\xi_1}{a_1} - h_2 (2 + a_2 h_2) \xi_2 + \frac{\xi_3}{a_3} \\ k_3 x_4 &= \frac{\xi_1}{a_1} + \frac{\xi_2}{a_2} - h_3 (2 + a_3 h_3) \xi_3. \end{aligned}$$

Da diese drei Ausdrücke für x_4 mit einander identisch sein müssen, so folgt:

$$- \frac{h_1 (2 + a_1 h_1)}{k_1} = \frac{1}{k_2 a_1} = \frac{1}{k_3 a_1},$$

also $k_2 = k_3$ und ebenso $k_2 = k_1$. Es sind also k_1, k_2, k_3 einander gleich und wir setzen dafür k. Dann folgt weiter

$$a_1 h_1 (2 + a_1 h_1) + 1 = (a_1 h_1 + 1)^2 = 0,$$

also $h_1 a_1 = -1$, und ebenso

$$h_1 = \frac{-1}{a_1}, \quad h_2 = \frac{-1}{a_2}, \quad h_3 = \frac{-1}{a_3}.$$

Demnach liefern die Formeln (13) übereinstimmend

$$k\, x_4 = \frac{\xi_1}{a_1} + \frac{\xi_2}{a_2} + \frac{\xi_3}{a_3}$$

oder

(14) $$k\,(a_1 x_1 + a_2 x_2 + a_3 x_3) = \frac{\xi_1}{a_1} + \frac{\xi_2}{a_2} + \frac{\xi_3}{a_3}.$$

Aus (11) aber folgt noch

(15) $$\lambda_1 = -\frac{a_2}{a_3},\quad \lambda_2 = -\frac{a_3}{a_1},\quad \lambda_3 = -\frac{a_1}{a_2}.$$

Aus (12) ergeben sich dann ferner die drei Relationen

$$-\frac{\xi_{42}}{\lambda_2} - \frac{\xi_{43}}{\lambda_3} = \frac{\xi_1}{a_1} + k\, a_1 x_1$$

$$-\frac{\xi_{43}}{\lambda_3} - \frac{\xi_{41}}{\lambda_1} = \frac{\xi_2}{a_2} + k\, a_2 x_2$$

$$-\frac{\xi_{41}}{\lambda_1} - \frac{\xi_{42}}{\lambda_2} = \frac{\xi_3}{a_3} + k\, a_3 x_3.$$

Daraus durch Addition mit Rücksicht auf (14)

$$\frac{\xi_{41}}{\lambda_1} + \frac{\xi_{42}}{\lambda_2} + \frac{\xi_{43}}{\lambda_3} = -\,k\,(a_1 x_1 + a_2 x_2 + a_3 x_3),$$

und folglich

(16) $$\begin{aligned} \frac{\xi_{41}}{\lambda_1} &= \frac{\xi_1}{a_1} - k\,(a_2 x_2 + a_3 x_3) \\ \frac{\xi_{42}}{\lambda_2} &= \frac{\xi_2}{a_2} - k\,(a_3 x_3 + a_1 x_1) \\ \frac{\xi_{43}}{\lambda_3} &= \frac{\xi_3}{a_3} - k\,(a_1 x_1 + a_2 x_2). \end{aligned}$$

Unbekannt ist in diesen Formeln noch die Constante k. Diese bestimmen wir aus der Bemerkung, dass wir das ganze bisher betrachtete Formelsystem vervierfachen können, indem wir an Stelle von x_4 treten lassen x_4, x_5, x_6, x_7.

Der Formel (10) entsprechend wollen wir diese vier Functionen linear durch x_1, x_2, x_3 ausdrücken in der Weise:

(17) $$\begin{aligned} x_4 &= a_{4,1} x_1 + a_{4,2} x_2 + a_{4,3} x_3 \\ x_5 &= a_{5,1} x_1 + a_{5,2} x_2 + a_{5,3} x_3 \\ x_6 &= a_{6,1} x_1 + a_{6,2} x_2 + a_{6,3} x_3 \\ x_7 &= a_{7,1} x_1 + a_{7,2} x_2 + a_{7,3} x_3, \end{aligned}$$

worin die Coëfficienten a als bekannt anzusehen sind. Dann bekommen wir aus (14) vier Relationen, wenn wir an Stelle von k vier verschiedene Constanten k_4, k_5, k_6, k_7 treten lassen:

$$(18)\quad \begin{aligned} k_4(a_{4,1}x_1 + a_{4,2}x_2 + a_{4,3}x_3) &= \frac{\xi_1}{a_{4,1}} + \frac{\xi_2}{a_{4,2}} + \frac{\xi_3}{a_{4,3}} \\ k_5(a_{5,1}x_1 + a_{5,2}x_2 + a_{5,3}x_3) &= \frac{\xi_1}{a_{5,1}} + \frac{\xi_2}{a_{5,2}} + \frac{\xi_3}{a_{5,3}} \\ k_6(a_{6,1}x_1 + a_{6,2}x_2 + a_{6,3}x_3) &= \frac{\xi_1}{a_{6,1}} + \frac{\xi_2}{a_{6,2}} + \frac{\xi_3}{a_{6,3}} \\ k_7(a_{7,1}x_1 + a_{7,2}x_2 + a_{7,3}x_3) &= \frac{\xi_1}{a_{7,1}} + \frac{\xi_2}{a_{7,2}} + \frac{\xi_3}{a_{7,3}}, \end{aligned}$$

und nun sind die Constanten k so zu bestimmen, dass von diesen vier Gleichungen die eine aus den drei anderen folgt. Die Bedingungen dafür kann man in symmetrischer Weise dadurch bilden, dass man vier Factoren l_4, l_5, l_6, l_7 einführt, deren Verhältnisse man aus den Gleichungen bestimmt:

$$(19)\quad \frac{l_4}{a_{4,i}} + \frac{l_5}{a_{5,i}} + \frac{l_6}{a_{6,i}} + \frac{l_7}{a_{7,i}} = 0, \quad i = 1, 2, 3,$$

und die dann auch den drei Gleichungen

$$(20)\quad k_4 l_4 a_{4,i} + k_5 l_5 a_{5,i} + k_6 l_6 a_{6,i} + k_7 l_7 a_{7,i} = 0, \quad i = 1, 2, 3$$

genügen müssen, woraus die Verhältnisse der k bestimmt sind. Ein gemeinschaftlicher Factor der vier Grössen k bleibt der Natur der Sache nach unbestimmt und kann beliebig angenommen werden. Hiernach können aus den Gleichungen (18) die Functionen ξ_1, ξ_2, ξ_3 rational bestimmt werden, und durch (16) sind dann auch die Functionen $\xi_{4i}, \xi_{5i}, \xi_{6i}, \xi_{7i}$ bestimmt.

Es fehlen noch sechs Doppeltangenten, die man durch geeignete Permutationen unter den Functionen des Systemes (1) erhalten kann. Damit ist der an die Spitze gestellte Satz I. bewiesen.

Um auch die Richtigkeit des Satzes II. einzusehen, braucht man nur unsere Analyse rückwärts zu verfolgen, indem man die Coëfficienten $a_{k,i}$ als unabhängige Variable ansieht. Dann sind durch die Gleichungen (18), (19), (20) die Functionen ξ_1, ξ_2, ξ_3

rational durch diese $a_{k,i}$ bestimmt, und aus (16) und (17) erhält man sodann $\xi_{4i}, \xi_{5i}, \xi_{6i}, \xi_{7i}, x_4, x_5, x_6, x_7$.

Durch Substitution der ξ_1, ξ_2, ξ_3 in die Gleichung (4) erhält man die Gleichung einer Curve vierter Ordnung, deren Coëfficienten rationale Functionen der $a_{k,i}$ sind, und die Discriminante dieser Gleichung kann nicht identisch verschwinden, weil man umgekehrt, wie wir gesehen haben, aus der Gleichung einer Curve vierter Ordnung ohne singulären Punkt ein Gleichungssystem (18), (19), (20) ableiten kann.

Aus den Gleichungen (18), (16) folgen dann auch die Formeln (7), und die daraus durch Vertauschung von 4 mit 5, 6, 7 hervorgehenden, woraus zu schliessen ist, dass x_4, x_5, x_6, x_7 zusammen mit x_1, x_2, x_3 ein vollständiges Siebener-System bilden.

§. 101.

Die Galois'sche Gruppe des Doppeltangentenproblems.

Die Sätze, die wir abgeleitet haben, sind ausreichend, um die Galois'sche Gruppe der algebraischen Gleichung zu bestimmen, von der die Doppeltangenten abhängen. Wir betrachten hierbei als Rationalitätsbereich den Körper, der aus allen rationalen Functionen der 14 Verhältnisse der Coëfficienten einer allgemeinen ternären Form 4ten Grades besteht, worin diese Coëfficienten als unabhängige Variable gelten. Die Gleichung 28sten Grades können wir uns dann etwa in der Weise gebildet denken, dass wir als Unbekannte die Abscissen der Schnittpunkte der Doppeltangenten mit einer beliebigen festen geraden Linie L betrachten. Durch die Wurzeln ξ dieser Gleichung, die wir die Doppeltangentengleichung nennen, sind dann die Doppeltangenten rational darstellbar.

Benutzt man ein Cartesisches Coordinatensystem x, y, dessen x-Axe die Linie L ist, so erhält die Gleichung einer Doppeltangente die Gestalt

$$(1) \qquad y = \Theta\,(x - \xi),$$

und die Doppeltangentengleichung kann gebildet werden, wenn $F(x, y) = 0$ die Gleichung der Curve vierter Ordnung ist, indem man die Bedingungen aufsucht, dass die Function von x

4ten Grades, $F[x, \Theta(x - \xi)]$ ein vollständiges Quadrat sei. Dies giebt zwei Gleichungen zwischen ξ und Θ, aus denen man durch Elimination von Θ die Doppeltangentengleichung erhält. Da zu jedem ξ nur ein Werth von Θ gehört (so lange sich nicht zwei Doppeltangenten auf der Linie L schneiden), so kann Θ rational durch ξ ausgedrückt werden, und zwar in einer Form

$$\Theta = \varphi(\xi), \tag{2}$$

die für jedes zusammengehörige Paar ξ, Θ gilt.

Die Wurzeln der Doppeltangentengleichung ordnen sich ebenso, wie die entsprechenden Doppeltangenten in Complexe, Siebener-Systeme u. s. w. Wir bezeichnen diese Wurzeln ebenso wie die Doppeltangenten in §. 99 durch das Symbol $[i\,k]$, worin i, k die Paare der Ziffern 1 bis 8 durchlaufen und $[i\,k] = [k\,i]$ ist.

Betrachten wir irgend zwei von den Doppeltangenten, p, q, als bekannt, so können wir auf rationalem Wege die Gleichung $u = 0$ eines Kegelschnittes daraus ableiten, der durch die vier Berührungspunkte dieser Doppeltangenten geht, und wir können also die Gleichung §. 96, (2)

$$f = p\,q\,v - u^2$$

in rationaler Form aufstellen. Dann giebt es nach §. 96, (4) unter der Kegelschnittschaar

$$v + 2\lambda u + \lambda^2 p\,q = 0$$

fünf, die in ein Linienpaar zerfallen, und wenn wir das Product

$$\prod^{\lambda} (v + 2\lambda u + \lambda^2 p\,q) = \Phi$$

bilden, über die fünf Wurzeln der Gleichung 5ten Grades, von der λ abhängt [§. 96, (6)], so ist dies Product gleichfalls rational durch die Coëfficienten von f und von p, q ausdrückbar. Dies Product ist aber eine Form 10ten Grades, die in zehn lineare Factoren zerfällt, die mit $p\,q$ zusammen einen Steiner'schen Complex bilden.

Die Coëfficienten in Φ können nun auch rational durch die beiden den p, q entsprechenden Wurzeln ξ_1, ξ_2 der Doppeltangentengleichung ausgedrückt werden, und wenn wir dann die Abscissen der Schnittpunkte der Linie L mit $\Phi = 0$ aufsuchen, so erhalten wir eine Gleichung 10ten Grades für ξ

$$X(\xi_1, \xi_2, \xi) = 0,$$

deren Wurzeln die zehn mit $\xi_1 \xi_2$ syzygetischen Wurzeln sind. Bedeutet ξ_3 eine von diesen, so ist also

(3) $$X(\xi_1, \xi_2, \xi_3) = 0,$$

und es folgt daraus der Satz

1. Es giebt eine rationale Function von drei Variablen $X(\xi_1, \xi_2, \xi_3)$, die verschwindet, wenn $\xi_1 \xi_2 \xi_3$ irgend ein syzygetisches Tripel von Wurzeln der Doppeltangentengleichung ist, und die nicht verschwindet, wenn $\xi_1 \xi_2 \xi_3$ ein azygetisches Tripel ist.

Nach §. 100 können durch ein vollständiges Siebener-System dieser Wurzeln

(4) $$\xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6, \xi_7$$

alle Wurzeln rational ausgedrückt werden, und zwar in der Weise, dass z. B.

(5) $$\xi_{12} = \Psi(\xi_1, \xi_2 \mid \xi_3, \xi_4, \xi_5, \xi_6, \xi_7)$$

eine Wurzel wird, wo Ψ eine rationale Function bedeutet, die sich nicht ändert, wenn ξ_1 und ξ_2 vertauscht oder wenn $\xi_3, \xi_4, \xi_5, \xi_6, \xi_7$ beliebig permutirt werden. Wird aber in (5) bei festgehaltener Function Ψ an Stelle von ξ_1, ξ_2 ein anderes Paar ξ_i, ξ_k gesetzt, so erhält man eine andere Wurzel ξ_{ik}. Die Wurzeln (4) sind auch mit [1 8], ... [7 8] und ξ_{ik} mit $[i\ k]$ zu bezeichnen.

Durch jede Permutation der Wurzeln (1) wird nach (2) das ganze System der Wurzeln $[i\ k]$ eine gewisse Permutation erfahren.

Ersetzt man aber das vollständige Siebener-System (4) durch ein anderes, so ergiebt die Formel (5) eine bestimmte andere Wurzel, und das ganze System der Wurzeln $[i\ k]$ wird einer zweiten Permutation unterworfen.

Es ist dann zunächst leicht zu beweisen:

2. Die Permutationsgruppe P der Wurzeln der Doppeltangentengleichung, die man erhält, wenn man in (4) und (5) an Stelle von $\xi_1, \xi_2, \ldots \xi_7$ alle vollständigen Systeme, jedes in jeder beliebigen Ordnung, setzt, ist die Galois'sche Gruppe der Doppeltangentengleichung.

Um dies nachzuweisen, haben wir Zweierlei zu zeigen:

a) Jede Permutation π der Wurzeln der Doppeltangentengleichung, die auf alle rationalen Gleichungen zwischen diesen Wurzeln anwendbar ist, gehört zu P.

Dies ergiebt sich so: Wenn π auf alle rationalen Gleichungen zwischen den Wurzeln anwendbar ist, so gilt dasselbe von den Potenzen von π. Nach 1. kann niemals durch π ein syzygetisches Tripel in ein azygetisches oder umgekehrt übergeführt werden; denn π ist, wenn $\xi_1\ \xi_2\ \xi_3$ ein syzygetisches Tripel ist, auf die Gleichung (3) anwendbar; also kann $\xi_1\ \xi_2\ \xi_3$ nicht in ein azygetisches Tripel übergehen. Und auch das Umgekehrte ist nicht möglich, weil sonst durch π^{-1} ein syzygetisches in ein azygetisches Tripel übergeführt würde. Daher geht auch durch π irgend ein vollständiges Siebener-System wieder in ein solches System in irgend welcher Anordnung über, und wenn man dann π auf alle Gleichungen von der Form (5) anwendet, so ergiebt sich eine Permutation der ξ_i, ξ_{ik}, die zu P gehört.

b) Jede rationale Gleichung zwischen den Wurzeln der Doppeltangentengleichung gestattet alle Permutationen der Gruppe P.

Eine rationale Relation zwischen den Wurzeln hat die Form

(6) $$\Phi\,(\xi_1, \ldots, \xi_7, \xi_{12}, \ldots, a \ldots) = 0,$$

worin Φ eine rationale Function ist, und $a \ldots$ die Verhältnisse der Coëfficienten von f bedeuten. Hierin kann man durch (5) die $\xi_{12}, \xi_{13}, \ldots$ rational durch $\xi_1, \xi_2, \ldots, \xi_7$ ausdrücken, und nach §. 100, II., nachdem die Curve f durch ein vollständiges Siebener-System ihrer Doppeltangenten rational bestimmt ist, lassen sich dann die a rational (mit nur numerischen Coëfficienten) durch die sieben Grössenpaare (2)

$$\xi_1, \Theta_1;\ \xi_2, \Theta_2;\ \ldots;\ \xi_7, \Theta_7$$

ausdrücken. Da diese aber ganz beliebig gegeben sein können, so muss die Gleichung (6) durch diese Substitutionen in eine Identität übergehen. Die Gleichung (6) muss also auch richtig bleiben, wenn man darin die $\xi_1, \xi_2, \ldots, \xi_7$ durch ein anderes Siebener-System oder auch durch dasselbe in anderer Ordnung ersetzt, und gleichzeitig unter den $\xi_{12}, \ldots$ die durch die Formel (5) vorgeschriebene Permutation vornimmt, d. h. wenn man unter den Wurzeln der Doppeltangentengleichung eine Permutation der Gruppe P ausführt.

§. 102.

Darstellung der Gruppe.

Der Grad der Gruppe P ist sofort anzugeben. Da es 288 vollständige Siebener-Systeme giebt, und da die Elemente eines solchen Systemes auf $\Pi(7)$ Arten permutirt werden können, so ist der Grad der Gruppe:

$$288\,\Pi(7) = 36\,\Pi(8) = 1451520.$$

Bei der Bildung der Permutationen der Wurzeln benutzen wir zweierlei Bezeichnung. Zunächst

$$(1) \qquad \xi_1, \xi_2, \ldots, \xi_7, \xi_{ik},$$

worin i, k von 1 bis 7 geht, und die einheitliche Bezeichnung $[i\,k]$, wobei i, k von 1 bis 8 geht, und wobei $\xi_1, \xi_2 \ldots$ durch $[1\,8], [2\,8], \ldots$ zu bezeichnen sind.

Wenn wir nun zwei Ziffern aus der Reihe $1, 2, \ldots, 7$ permutiren, z. B. 1 mit 2, so geht ξ_1 in ξ_2 über, und nach der Definition §. 99 bleibt ξ_{12} ungeändert, ξ_{13} geht in ξ_{23} über u. s. f.

Wenn wir also in der Reihe der Wurzeln $[i\,k]$ die Ziffern 1 bis 7 beliebig permutiren, so erhalten wir lauter Permutationen der Gruppe P.

Nun haben wir im §. 100 gesehen, dass bei der Anordnung in syzygetische und azygetische Tripel und in Folge dessen auch in Complexe und vollständige Systeme die Ziffer 8 mit den übrigen Ziffern 1 bis 7 vollständig gleichberechtigt auftritt, und da die Zuordnung der Wurzel ξ_{ik} zu dem Paare $\xi_i \xi_k$ [durch die Formel §. 101, (5)] nach §. 99 nur von dieser Anordnung abhängt, so können wir auch die Ziffern $1, 2, \ldots, 7, 8$ permutiren, ohne dass wir aus der Gruppe P herauskommen. Es ist also in P ein Theiler enthalten, der mit der symmetrischen Gruppe der Permutationen von acht Elementen isomorph ist, der also den Index 36 hat und den wir mit S bezeichnen wollen.

Um die noch fehlenden Permutationen von P zu bestimmen, lassen wir an Stelle des Siebener-Systemes $\xi_1, \ldots, \xi_7$ ein neues vom Typus $\triangle \,\Psi$ treten, etwa so:

$$(2) \qquad \begin{pmatrix} [1\,8], & [2\,8], & [3\,8], & [4\,8], & [5\,8], & [6\,8], & [7\,8] \\ [2\,3], & [3\,1], & [1\,2], & [4\,8], & [5\,8], & [6\,8], & [7\,8] \end{pmatrix},$$

und bezeichnen die hierdurch bedingte Permutation in doppelter Weise mit

(3) $$\Pi_{1,2,3,8} = \Pi_{4,5,6,7},$$

indem wir festsetzen, dass $\Pi_{\alpha_1 \alpha_2 \alpha_3 \alpha_4}$ und $\Pi_{\beta_1 \beta_2 \beta_3 \beta_4}$ dasselbe bedeuten sollen, wenn $\beta_1, \beta_2, \beta_3, \beta_4$ irgend eine Permutation von $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ ist, oder wenn $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1, \beta_2, \beta_3, \beta_4$ zusammen alle acht Ziffern umfassen.

Durch dies Zeichen ist die Vertauschung (2) eindeutig bezeichnet, und die Anzahl der verschiedenen Permutationen dieser Art beträgt genau 35, so dass wir die ganze Gruppe P durch die Nebengruppen so darstellen können:

(4) $$P = S + \Sigma\, S\, \Pi_{\alpha_1 \alpha_2 \alpha_3 \alpha_4},$$

worin $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ alle Systeme von vier Ziffern aus der Reihe 1, 2, ..., 8 durchlaufen, wobei eine beliebige Ziffer, z. B. $\alpha_4 = 8$, festgehalten werden kann.

Um den Einfluss von $\Pi_{1,2,3,8}$ auf irgend eine Wurzel $[i\, k]$ zu erkennen, genügt es, die drei Wurzeln [1 2], [1 4], [4 5] zu betrachten, weil 1, 2, 3 einerseits, 4, 5, 6, 7 andererseits ganz gleichartig in $\Pi_{1,2,3,8}$ vorkommen.

Diese Vertauschungen erhält man einfach aus der Bemerkung, dass [1 2], [1 4] nach §. 99 die in dem Complex

(5) [2 8][1 2], [3 8][1 3], [4 8][1 4], [5 8][1 5], [6 8][1 6], [7 8][1 7]

mit [2 8] und [4 8] verbundenen Wurzeln sind, und dass ebenso [4 5] die mit [5 8] verbundene Wurzel in dem Complexe

(6) [1 8][1 4], [2 8][2 4], [3 8][3 4], [5 8][5 4], [6 8][6 4], [7 8][7 4]

ist. Durch die Vertauschung (2) gehen aber die Complexe (5) und (6) in folgende über, wie man leicht aus der Darstellung der Complexe im §. 99 findet [der Complex (5) bleibt als Ganzes ungeändert]:

[3 1][3 8], [2 1][2 8], [4 8][1 4], [5 8][5 1], [6 8][6 1], [7 8][7 1]

[2 3][1 4], [3 1][2 4], [1 2][3 4], [5 8][6 7], [6 8][5 7], [7 8][5 6],

woraus man folgende durch $\Pi_{1,2,3,8}$ bewirkte Vertauschungen erhält:

(7)
[1 2], [1 4], [4 5]
[3 8], [1 4], [6 7].

Aus (2) und (7) lässt sich nun folgende allgemeine und einfache Regel ableiten.

3. Bedeuten $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1, \beta_2, \beta_3, \beta_4$ zusammen alle acht Ziffern, so hat man, um den Einfluss von

$$\Pi_{\alpha_1 \alpha_2 \alpha_3 \alpha_4} = \Pi_{\beta_1 \beta_2 \beta_3 \beta_4}$$

auf irgend eine Wurzel $[\mu\ \nu]$ zu bestimmen, zu unterscheiden, ob μ, ν beide unter den α oder beide unter den β, oder ob die Ziffer μ unter den α, ν unter den β vorkommt. In den ersten Fällen geht $[\mu\ \nu]$ in $[\mu'\ \nu']$ über, wenn μ, ν, μ', ν' entweder alle α oder alle β bedeuten; im dritten Falle bleibt $[\mu\ \nu]$ ungeändert.

In allen Fällen sind die Permutationen $\Pi_{\alpha_1 \alpha_2 \alpha_3 \alpha_4}$ nur vom 2ten Grade, führen also bei einmaliger Wiederholung zur Identität zurück.

Damit ist die Gruppe P vollständig bestimmt und dargestellt, und um die Gesetze der Composition in P festzustellen, sind nur noch wenige Formeln nöthig, die sich aus der oben aufgestellten Regel leicht ergeben. Dabei ist zu bemerken, dass man zwei von einander verschiedene der Permutationen $\Pi_{\alpha_1 \alpha_2 \alpha_3 \alpha_4}$ immer so annehmen kann, dass sie im Index zwei oder drei Ziffern gemein haben, da man, wenn sie nur eine Ziffer gemein haben, für den Index der einen seine Ergänzung nehmen kann.

Es möge nun

$$\sigma = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8 \\ \alpha_1, & \alpha_2, & \alpha_3, & \alpha_4, & \alpha_5, & \alpha_6, & \alpha_7, & \alpha_8 \end{pmatrix}$$

irgend eine Permutation der acht Ziffern sein und (α, β) die Transposition der beiden Ziffern α und β, also ein Element aus S, bedeuten. Dann ist

$$(8) \qquad \Pi_{1,2,3,4}\, \sigma = \sigma\, \Pi_{\alpha_1 \alpha_2 \alpha_3 \alpha_4},$$

$$(9) \qquad \Pi_{1,2,3,4}\, \Pi_{1,2,3,4} = 1,$$

$$(10) \qquad \Pi_{1,2,3,4}\, \Pi_{1,2,3,5} = (4,5)\, \Pi_{1,2,3,4},$$

$$(11) \qquad \Pi_{1,2,3,4}\, \Pi_{1,2,5,6} = (1,2)\,(3,4)\,(5,6)\,(7,8)\, \Pi_{1,2,7,8}.$$

Man beweist diese Formeln leicht nach der Regel 3., wenn man die einzelnen Fälle durchgeht, wobei natürlich nur eine ganz kleine Zahl von Typen zu betrachten sind; so geht z. B. [1 4] durch $\Pi_{1,2,3,4}$ in [2 3], dies durch $\Pi_{1,2,3,5}$ in [1 5] über, und [1 5] wird durch $\Pi_{1,2,3,4}$ nicht mehr geändert, folglich bewirkt

$$(12) \qquad \Pi_{1,2,3,4}\, \Pi_{1,2,3,5}\, \Pi_{1,2,3,4}$$

die Vertauschung von [1 4] mit [1 5] in Uebereinstimmung mit der Formel (10). Ebenso leicht erkennt man, dass z. B. [1 2] durch (12) nicht geändert wird.

§. 103.

Einfachheit der Gruppe des Doppeltangentenproblems.

Die Darstellung der Gruppe P, die wir im vorigen Paragraphen entwickelt haben, liefert uns nun einen ganz einfachen Beweis dafür, dass diese Gruppe keinen Normaltheiler hat, also nach unserer früher gebrauchten Ausdrucksweise einfach ist, woraus dann folgt, dass die Gruppe nicht durch Adjunction von Irrationalitäten mit kleinerer Gruppe, also beispielsweise nicht durch cyklische Gleichungen erniedrigt werden kann.

Wir stellen P in der Form (4), §. 102, dar:

(1) $$P = S + \Sigma\, S\, \Pi_{\alpha_1, \alpha_2, \alpha_3, \alpha_4},$$

worin S die ganze Gruppe aller Permutationen von acht Ziffern ist. Die Gruppe S hat einen Normaltheiler S' vom Index 2, nämlich die alternirende Gruppe der acht Ziffern, die ihrerseits einfach ist, und jeder Normaltheiler von S, der nicht aus der einzigen identischen Permutation besteht, muss die ganze Gruppe S' enthalten. Wir setzen

(2) $$S = S' + S'',$$

worin $S'' = S'\sigma$ ist, wenn σ irgend eine Permutation der zweiten Art, z. B. eine Transposition bedeutet.

Wir nehmen jetzt an, es sei Q ein Normaltheiler von P, der nicht aus der einzigen identischen Substitution besteht.

Der grösste gemeinschaftliche Theiler von Q und S ist dann ein Normaltheiler von S, und muss daher, wenn er nicht die identische Gruppe ist, die Gruppe S' enthalten. Daraus folgt:

1. Wenn Q eine nicht identische Permutation aus S enthält, so enthält Q die ganze Gruppe S'.

Wir beweisen sodann, dass Q, wenn es die Gruppe S' enthält, mit P identisch sein muss.

Wenn nämlich Q die ganze Gruppe S' enthält, so enthält

es als Normaltheiler von P auch, wenn $(4,5,6)$ ein dreigliedriger Cyklus aus S' ist [nach §. 102, (8), (10)]:

$$\Pi_{1,2,3,5}\,(5,4,6)\,\Pi_{1,2,3,5} = (5,4,6)\,\Pi_{1,2,3,4}\,\Pi_{1,2,3,5}$$
$$= (5,4,6)\,(4,5)\,\Pi_{1,2,3,4},$$

und folglich auch

$$S'(4,5)\,\Pi_{1,2,3,4} = S''\,\Pi_{1,2,3,4}.$$

Ist nun

$$\sigma = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8 \\ \alpha_1, & \alpha_2, & \alpha_3, & \alpha_4, & \alpha_5, & \alpha_6, & \alpha_7, & \alpha_8 \end{pmatrix}$$

eine Permutation aus S, in der $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ beliebig gegeben sind, so kann man die Anordnung der $\alpha_5, \alpha_6, \alpha_7, \alpha_8$ noch so wählen, dass σ nach Belieben zu S' oder zu S'' gehört. Wählt man σ in S' und beachtet, dass dann $S'' = S''\sigma^{-1}$ ist, so ergiebt sich, dass auch

$$S''\sigma^{-1}\,\Pi_{1,2,3,4}\,\sigma = S''\,\Pi_{\alpha_1,\alpha_2,\alpha_3,\alpha_4}$$

in Q enthalten sein muss. Nun ist aber auch

$$\Pi_{1,2,3,4}\,(3,5)\,(4,6)\,\Pi_{1,2,3,4} = (3,5)(4,6)\,\Pi_{1,2,5,6}\,\Pi_{1,2,3,4}$$
$$= (3,5)(4,6)(1,2)(3,4)(5,6)(7,8)\,\Pi_{1,2,7,8}$$
$$= (1,2)(3,6)(4,5)(7,8)\,\Pi_{1,2,7,8},$$

und da $(1,2)\,(3,6)\,(4,5)\,(7,8)$ zu S' gehört, so enthält Q auch $S'\Pi_{1,2,7,8}$, und folglich, wie oben, alle $S'\Pi_{\alpha_1,\alpha_2,\alpha_3,\alpha_4}$, also auch alle $S\,\Pi_{\alpha_1\alpha_2\alpha_3\alpha_4}$, und mithin auch

$$S\,\Pi_{\alpha_1,\alpha_2,\alpha_3,\alpha_4}\,\Pi_{\alpha_1,\alpha_2,\alpha_3,\alpha_4} = S,$$

d. h. Q umfasst die ganze Gruppe P. Daraus folgt in Verbindung mit 1.:

2. Wenn ein Normaltheiler Q von P ausser der identischen Permutation noch irgend eine Permutation mit S gemein hat, so ist Q mit P identisch.

Es kann nun ferner die Frage sein, ob Q eine Permutation aus einer der Nebengruppen von (1), also ein Element von der Form $\sigma\Pi_{1,2,3,4}$ enthalten kann, ohne mit P identisch zu sein. Ist zunächst $\sigma = 1$, enthält also Q das Element $\Pi_{1,2,3,4}$, so enthält es als Normaltheiler von P auch alle anderen $\Pi_{\alpha_1\alpha_2\alpha_3\alpha_4}$, wie aus der Formel §. 102, (8) zu ersehen ist, und damit auch $\Pi_{1,2,3,4}\,\Pi_{1,2,3,5}\,\Pi_{1,2,3,4} = (4,5)$, und ist also nach 2. mit P identisch.

Ist aber σ von 1 verschieden, so kann man ein Ziffernpaar α, β, beide unter den 1, 2, 3, 4 oder beide unter den 5, 6, 7, 8, so wählen, dass die Transposition

$$\sigma (\alpha, \beta) \sigma^{-1} = (\alpha', \beta')$$

von (α, β) verschieden ist. Denn nimmt man zunächst für α eine durch σ^{-1} veränderte Ziffer, so ist α' von α verschieden (Bd. I, §. 154, 6.), wählt man dann für β eine Ziffer, die durch σ^{-1} nicht in α übergeht und die mit α zugleich in der ersten oder in der zweiten Hälfte der acht Ziffern vorkommt, die gewiss immer existirt, weil nur eine Ziffer durch σ^{-1} in α übergeht, so ist (α', β') von (α, β) verschieden. Dann folgt aber, dass in der Gruppe Q das Element $(\alpha, \beta)\, \sigma\, \Pi_{1,2,3,4}\, (\alpha, \beta)$, und folglich auch [nach §. 102, (8), (9)]

$$(\alpha, \beta)\, \sigma\, \Pi_{1,2,3,4}\, (\alpha, \beta)\, \Pi_{1,2,3,4}\, \sigma^{-1} = (\alpha, \beta)\, \sigma\, (\alpha, \beta)\, \sigma^{-1} = (\alpha, \beta)(\alpha', \beta')$$

vorkommt, und dies ist eine von der Identität verschiedene Permutation aus S. Damit ist also bewiesen:

3. Die Gruppe P der Doppeltangentengleichung ist einfach.

Als specielle Anwendung können wir hervorheben, dass die Gruppe P unter den 28 Wurzeln der Doppeltangentengleichung nur Permutationen der ersten Art bewirken kann, und dass folglich die Discriminante dieser Gleichung ein Quadrat ist.

Bezeichnen wir nämlich für den Augenblick mit G die Gruppe aller Permutationen der 28 Wurzeln und mit A die darin als Normaltheiler enthaltene alternirende Gruppe, so ist der grösste gemeinschaftliche Theiler von A und P ein Normaltheiler von P und muss also mit P identisch sein; d. h. P ist in A enthalten.

Wenn man die Gruppe der Permutationen aufsucht, die eine der Wurzeln der Doppeltangentengleichung, etwa [1 2], ungeändert lassen, so findet man eine Gruppe, die für die übrigen 27 Wurzeln noch transitiv ist[1]).

---

[1]) Diese Gruppe ist nach einem geometrischen Satze von Geiser isomorph mit der Gruppe der Gleichung 27sten Grades, von der die Lösung des Problems der 27 Geraden auf einer Fläche dritter Ordnung abhängt. (Mathem. Annalen, Bd. I.).

Um dies nachzuweisen, genügt es zu zeigen, dass durch die Permutationen dieser Gruppe irgend eine Wurzel, etwa [1 3], in jede andere (mit Ausnahme von [1 2]) übergehen kann. Nun geht aber [1, 3] durch Permutationen der Gruppe S, durch die 1, 2 ungeändert bleiben, in [1 4], . . ., [1 8] über; ebenso [2 3] in [2 4], . . ., [2 8]. Es bleibt also noch zu zeigen, dass man [1 3] auch in [2 3] und in [4 5] überführen kann. Dies zeigt aber der Anblick der drei folgenden vollständigen Siebener-Systeme:

[1 2] [1 3] [1 4] [1 5] [1 6] [1 7] [1 8]
[1 2] [2 3] [2 4] [2 5] [2 6] [2 7] [2 8]
[1 2] [4 5] [3 4] [3 5] [1 6] [1 7] [1 8].

Die Gruppe P ist hiernach zweifach transitiv. Sie kann aber nicht mehr als zweifach transitiv sein. Denn lässt man zwei Wurzeln ungeändert, so kann eine mit diesen beiden syzygetische Wurzel nicht in eine azygetische übergeführt werden. Durch Adjunction von zwei Wurzeln wird die Doppeltangentengleichung reducibel. Es löst sich ein Factor 10ten Grades ab, dessen Wurzeln mit den beiden gegebenen einen Steiner'schen Complex bilden (die Function X im Satze 1., §. 101).

Unter den Divisoren der Gruppe P ist besonders die Gruppe S vom Index 36 bemerkenswerth. Diese Gruppe ist noch transitiv, weil durch sie [1 2] in jede beliebige Wurzel $[\varkappa\, \lambda]$ übergeführt werden kann. Sie ist aber nur noch einfach transitiv, weil bei festgehaltenem [1 2] die Wurzel [1 3] nicht mehr in [4 5] übergehen kann.

Durch Adjunction einer Wurzel einer Gleichung 36sten Grades wird also die Gruppe der Doppeltangentengleichung auf die Gruppe einer allgemeinen Gleichung 8ten Grades reducirt.

Setzt man z. B.

$$v_1 = [1\,2]\,[1\,3]\,[1\,4]\,[1\,5]\,[1\,6]\,[1\,7]\,[1\,8],$$

und definirt entsprechend $v_2, v_3, \ldots, v_8$, so ist jede symmetrische Function dieser acht Grössen, z. B.

$$u = v_1 + v_2 + v_3 + v_4 + v_5 + v_6 + v_7 + v_8,$$

Wurzel einer Gleichung 36sten Grades. Adjungirt man dem Problem die Grösse u, so werden die $v_1, v_2, \ldots, v_8$ die Wurzeln einer Gleichung 8ten Grades, die keinen Affect hat.

§. 104.
Realität der Doppeltangenten.

Wir wollen noch die Frage erörtern, wie sich bei einer reellen Curve vierter Ordnung ohne singulären Punkt die Doppeltangenten in Bezug auf ihre Realität verhalten können. Wir nehmen also jetzt die Coëfficienten der Gleichung der Curve vierter Ordnung reell an, d. h. wir setzen einen reellen Rationalitätsbereich voraus.

Wenn dann eine Doppeltangente ξ imaginär ist, so muss auch die conjugirte Gerade ξ' Doppeltangente sein.

Wenn wir in einer rationalen Gleichung zwischen den Wurzeln der Doppeltangentengleichung jede imaginäre Wurzel durch die conjugirte ersetzen, so entsteht wieder eine richtige Gleichung. Es folgt daraus, dass zu syzygetischen oder azygetischen Systemen vom Doppeltangenten conjugirte Systeme desselben Charakters gehören, die man erhält, wenn man überall i durch $-i$ ersetzt.

Ein Steiner'scher Complex C geht daher durch Uebergang von i zu $-i$ in einen Steiner'schen Complex C' über und wir unterscheiden zwei Fälle:

Ist C mit C' identisch, so nennen wir $C = C'$ einen reellen Complex.

Ist aber C von C' verschieden, so bilden sie ein conjugirtes Complexpaar.

Die Paare eines reellen Complexes bestehen entweder aus zwei reellen Doppeltangenten oder es sind conjugirte Paare ξ, ξ', oder sie enthalten zwei nicht conjugirte imaginäre Doppeltangenten ξ, η. Im letzteren Falle muss dann im Complex auch das aus den conjugirten Doppeltangenten ξ', η' gebildete Paar vorkommen. Zwei solche Paare (ξ, η), (ξ', η') wollen wir ein conjugirtes Doppelpaar nennen.

Niemals kommt in einem reellen Complexe eine reelle Wurzel x mit einer imaginären ξ gepaart vor, weil sonst neben dem Paare (x, ξ) auch das conjugirte Paar (x, ξ') in demselben Complexe vorkommen müsste, was unmöglich ist, da diese beiden Paare ein gemeinschaftliches Element x enthalten würden.

Ein Aronhold'sches Siebener-System S geht durch Vertauschung aller seiner Elemente mit den conjugirten in ein eben-

solches System S' über, und wir nennen ein solches System **reell**, wenn S mit S' identisch ist. Ein reelles Siebener-System enthält daher zu jeder in ihm vorkommenden Wurzel ξ die conjugirte ξ', und muss folglich wenigstens eine, immer aber eine ungerade Anzahl von reellen Doppeltangenten enthalten.

Wir leiten jetzt der Reihe nach die Hauptsätze ab:

1. Es können nicht alle Doppeltangenten imaginär sein.

Es sei nämlich ξ, ξ' ein conjugirtes Paar und η eine dritte imaginäre Doppeltangente, so dass die drei ξ, ξ', η **azygetisch** sind. (Dies wäre sicher möglich, wenn alle Doppeltangenten imaginär wären.) Ist η' zu η conjugirt, so haben wir die beiden azygetischen Tripel:

$$\xi, \xi', \eta; \quad \xi, \xi', \eta'.$$

Da hiernach in dem durch das Paar $\xi\,\eta$ bestimmten Steiner'schen Complexe ξ' nicht vorkommt, so ist dieser Complex imaginär.

Wir stellen ihn mit seinem conjugirten Complexe zusammen:

$$(1) \qquad \begin{array}{ll} 1) & \xi\,\eta,\ \xi_1\,\eta_1,\ \xi_2\,\eta_2,\ \xi_3\,\eta_3,\ \xi_4\,\eta_4,\ \xi_5\,\eta_5 \\ 2) & \xi'\eta',\ \xi_1'\,\eta_1',\ \xi_2'\,\eta_2',\ \xi_3'\,\eta_3',\ \xi_4'\,\eta_4',\ \xi_5'\,\eta_5', \end{array}$$

indem wir unter ξ_i', η_i' die zu ξ_i, η_i conjugirten Elemente verstehen, so dass, falls ξ_i reell ist, $\xi_i = \xi_i'$ zu setzen ist, und umgekehrt auch aus $\xi_i = \xi_i'$ folgt, dass ξ_i reell ist.

Es sind nun zwei Möglichkeiten zu unterscheiden. Wenn **erstens** die Complexe 1), 2) ein syzygetisches Paar bilden (§. 97), so haben sie vier syzygetische Elemente gemein. Darunter können ξ, η, ξ', η' nicht vorkommen, und wir beschränken daher die Allgemeinheit nicht, wenn wir annehmen, es seien $\xi_1, \eta_1, \xi_2, \eta_2$ die gemeinschaftlichen Elemente. Diese können in ihrer Gesammtheit aber nicht verschieden sein von $\xi_1', \eta_1', \xi_2', \eta_2'$, da der Uebergang zu den accentuirten Buchstaben, d. h. zu den conjugirt imaginären Grössen, wodurch 1) in 2) übergeht, überall gestattet ist.

Nun ist die Annahme $\xi_1 = \eta_1'$ ausgeschlossen, weil daraus $\xi_1' = \eta_1$ folgen würde und 1) von 2) nicht verschieden wäre.

Ist $\xi_1 = \xi_1'$, so ist ξ_1 **reell**.

Ist aber $\xi_1 = \xi_2'$, $\xi_2 = \xi_1'$, so ist $\eta_1 = \eta_1'$, also η_1 **reell**, und davon ist die Annahme $\xi_1 = \eta_2'$, $\xi_1' = \eta_2$, $\xi_2 = \xi_2'$ nicht wesentlich verschieden.

Dieser Fall führt also immer auf eine reelle Doppeltangente.

Wenn aber zweitens das Complexpaar 1), 2) azygetisch ist, so enthält jedes Paar des einen Complexes ein Element, was auch im anderen Complexe vorkommt, und ein Element, was im anderen nicht vorkommt. Kommt also etwa η im Complexe 2) vor, so können wir, ohne Beeinträchtigung der Allgemeinheit $\eta = \eta_1'$, $\eta' = \eta_1$ annehmen, und erhalten folgende Paare in 1) und 2)

$$(2) \qquad \begin{array}{ll} 1) & \xi\,\eta, \quad \xi_1\,\eta' \\ 2) & \xi_1'\,\eta, \quad \xi'\,\eta' \end{array}.$$

Wenn ferner η_2 in 1) und 2) vorkommt, so kann η_2 nicht gleich ξ_2' sein, weil sonst 1) das Paar $\xi_2\,\xi_2'$ enthielte und folglich reell wäre.

Wenn $\eta_2 = \eta_2'$ ist, so ist η_2 reell. Ist aber η_2 gleich einem Element der drei letzten Paare von 2), so können wir es ohne Beschränkung $= \eta_3'$ annehmen, also $\eta_2 = \eta_3'$, $\eta_3 = \eta_2'$.

Dann sind aber nach dem Satze §. 96, 3. sowohl η, η_2, η_2' als η, η', η_2 azygetisch. Die beiden Paare $\eta\,\eta_2$, $\eta'\,\eta_2'$ bestimmen zwei Complexe, deren zweiter weder η noch η_2 enthält, und die daher ein syzygetisches Paar bilden. Damit sind wir auf die erste Annahme zurückgeführt und unser Satz 1. ist bewiesen.

Es giebt also immer mindestens zwei reelle Doppeltangenten.

2. Es giebt immer mindestens ein System von vier reellen syzygetischen Doppeltangenten.

Beim Beweise dieses Satzes gehen wir aus von einem nach 1. immer existirenden reellen Paare $x\,y$, und betrachten den reellen Complex, der durch dies Paar bestimmt ist. Da die conjugirten Doppelpaare je zwei Paare sind, so muss unter den sechs Paaren dieses Complexes entweder ein zweites reelles Paar vorkommen, und dann trifft der Satz 2. zu, oder er muss ein conjugirtes Paar $\xi\,\xi'$ enthalten.

Im letzteren Falle betrachten wir das durch diese beiden Paare bestimmte syzygetische Complextripel, in dem alle 28 Doppeltangenten vorkommen (§. 97, 4.):

$$\begin{array}{llll} 1) & x\,y, & \xi\,\xi' & \\ 2) & x\,\xi, & y\,\xi', & \xi_1\,\eta_1 \\ 3) & x\,\xi', & y\,\xi, & \xi_1'\,\eta_1', \end{array}$$

von denen die beiden letzten conjugirt imaginär sind, und folglich, da sie ausser x, y, ξ, ξ' kein gemeinschaftliches Element haben, nur noch imaginäre Paare enthalten, von denen wir eins, $\xi_1 \eta_1$, nebst dem dazu conjugirten $\xi'_1 \eta'_1$ mit aufgeführt haben.

Es genügt demnach, wenn wir die Existenz von einer weiteren reellen Doppeltangente beweisen können. Denn diese muss dann in 1) vorkommen und muss in diesem Complexe zu einem reellen Paare gehören.

Jetzt bilden wir noch die beiden conjugirten Complexe:

$$4) \quad x\,\xi_1, \quad \xi\,\eta_1$$
$$5) \quad x\,\xi'_1, \quad \xi'\,\eta'_1,$$

in denen y gewiss nicht vorkommt, da sonst x, ξ, y azygetisch wären (§. 96, 3.). Aus demselben Grunde kommt ξ nicht in 5) und ξ' nicht in 4) vor.

Wenn nun zunächst die Complexe 4) und 5) syzygetisch sind, so muss ξ_1 in 5) und ξ'_1 in 4) vorkommen, und wenn 4) das Paar $p\,\xi'_1$ enthält, so muss in 5) das Paar $p\,\xi_1$ vorkommen. Es ist also p mit seinem conjugirten Elemente identisch, d. h. reell.

Wenn zweitens die Complexe 4) und 5) azygetisch sind, so kommen ξ_1, ξ nicht in 5) vor, und es muss η_1 in 5) enthalten sein. Wenn η_1 in 5) mit einem imaginären Elemente ξ'_2 gepaart ist, und wenn in 4) noch ein weiteres imaginäres Paar $\xi_3\,\eta_3$ vorkommt, so setzen sich diese Complexe in folgender Weise fort:

$$4) \quad x\,\xi_1, \quad \xi\,\eta_1, \quad \xi_2\,\eta'_1, \quad \xi_3\,\eta_3, \quad \xi'_3\,\eta_4$$
$$5) \quad x\,\xi'_1, \quad \xi'\,\eta'_1, \quad \xi'_2\,\eta_1, \quad \xi'_3\,\eta'_3, \quad \xi_3\,\eta'_4,$$

worin auch η_4 imaginär ist, und durch die accentuirten Buchstaben immer die conjugirten Elemente zu den unaccentuirten verstanden sind. Die beiden Complexe enthalten dann nur noch je ein Paar $\xi_5\,\eta_5$, $\xi'_5\,\eta'_5$, die ein gemeinschaftliches Element enthalten müssen. Es kann aber nicht $\xi_5 = \eta'_5$ sein, weil sonst auch $\xi'_5 = \eta_5$, und mithin beide Paare identisch wären. Also muss $\xi_5 = \xi'_5$ (oder $\eta_5 = \eta'_5$) sein; d. h. eine dieser beiden Doppeltangenten ist reell, und damit ist unser Satz 2. bewiesen.

3. Wenn ausser den vier reellen Doppeltangenten x, y, p, q, deren Existenz der Satz 2. behauptet, noch eine weitere vorhanden ist, so existiren acht reelle Doppeltangenten, die in einem Steiner'schen Complexe vier Paare bilden.

Wir bilden das reelle syzygetische Complextripel, in dem alle Doppeltangenten vorkommen müssen:

$$\begin{array}{ll} 1) & xy,\ pq \\ 2) & xp,\ yq \\ 3) & xq,\ yp. \end{array}$$

Ist eine fünfte reelle Doppeltangente r vorhanden, so können wir annehmen, sie komme im Complexe 1) vor. Dann muss aber dieser Complex ein drittes reelles Paar rs enthalten, und entweder ein viertes reelles Paar, in welchem Falle der Satz 3. schon zutrifft, oder ein conjugirtes Paar $\varrho\varrho'$.

Enthält der Complex 2) nicht lauter reelle Doppeltangenten, ein Fall, in dem gleichfalls der Satz 3. zutreffen würde, so muss in 2) ein imaginäres Paar $\xi\eta$ vorkommen, und danach betrachten wir also die folgenden Complexe:

$$\begin{array}{ll} 1) & xy,\ pq,\ rs,\ \varrho\varrho' \\ 2) & xp,\ yq,\ \xi\eta \\ 4) & xr,\ ys. \end{array}$$

Die beiden Complexe 2), 4) sind aber azygetisch, da z. B. r in 2) nicht vorkommt [weil es in 1) vorkommt]. Folglich kann 4) auch nur eine der beiden ξ, η enthalten, und folglich können, da der Complex 4) reell ist, ξ, η nicht conjugirt sein. Es ergiebt sich daraus für 2) und 4) je ein conjugirtes Doppelpaar, und wir haben:

$$\begin{array}{ll} 2) & xp,\ yq,\ \xi\eta,\ \xi'\eta' \\ 4) & xr,\ ys,\ \xi\zeta,\ \xi'\zeta'. \end{array}$$

worin ζ, ζ' wieder ein Paar conjugirter Doppeltangenten bedeutet.

Nun bilden wir den sowohl mit 2) als mit 4) syzygetischen reellen Complex

$$5) \quad \xi\xi',\ \eta\eta',\ \zeta\zeta',$$

der keines der Elemente x, y, p, q, r, s enthalten kann, und ferner die beiden conjugirt imaginären Complexe

$$\begin{array}{ll} 6) & x\xi,\ p\eta,\ r\zeta \\ 7) & x\xi',\ p\eta',\ r\zeta', \end{array}$$

und 5), 6), 7) bilden ein azygetisches Tripel. y, q, s kommen in 6) und 7) nicht vor, denn sonst müssten sie mit je zweien der x, p, r azygetisch sein, was nach 2) und 4) unmöglich ist.

Es ist also jeder der Complexe 6), 7) azygetisch mit dem Complexe 1), und es muss also eine und nur eine der beiden Doppeltangenten ϱ, ϱ' in 6) vorkommen; ist dies ϱ, so ist ϱ' in 7) enthalten. Ist $\varrho\,\sigma$ ein Paar von 6), so ist σ von seinem conjugirten σ' verschieden, weil sonst $\sigma\,\varrho'$ in 7) und folglich $\varrho\,\varrho'$ in 5) vorkommen müsste, was nicht der Fall ist. Also haben wir, wenn τ, τ' zwei weitere conjugirt imaginäre Doppeltangenten sind, die Complexe:

$$6) \quad x\,\xi,\ p\,\eta,\ r\,\zeta,\ \varrho\,\sigma,\ \sigma'\,\tau$$
$$7) \quad x\,\xi',\ p\,\eta',\ r\,\zeta',\ \varrho'\sigma',\ \sigma\,\tau'.$$

Ist $t\,\lambda$ das letzte Paar des Complexes 6), so kommt das Paar $t'\,\lambda'$ in 7) vor, und diese beiden Paare müssen ein gemeinsames Element enthalten. Da aber λ nicht gleich t' sein kann, weil sonst beide Paare identisch wären, so muss $t = t'$ (oder $\lambda = \lambda'$, was nicht wesentlich verschieden ist) sein; es ist also t reell, und es wird:

$$6) \quad x\,\xi,\ p\,\eta,\ r\,\zeta,\ \varrho\,\sigma,\ \sigma'\tau,\ t\,\lambda$$
$$7) \quad x\,\xi',\ p\,\eta',\ r\,\zeta',\ \varrho'\sigma',\ \sigma\,\tau',\ t\,\lambda'.$$

Jetzt kehren wir zu dem syzygetischen Complextripel 1), 2), 3) zurück. Da wir aus 6) schliessen, dass $x\,p\,t$ und $x\,r\,t$ azygetisch sind, so kann t weder in 2) noch in 3) vorkommen, und muss also in 1) enthalten sein. Da aber 1) ein reeller Complex ist, so muss darin t mit einer reellen Doppeltangente u gepaart erscheinen, und der Complex 1) wird

$$x\,y,\ p\,q,\ r\,s,\ t\,u,$$

wodurch unser Satz 3. bewiesen ist.

4. Wenn in einem Complexe fünf reelle Paare vorkommen, so sind alle Doppeltangenten reell.

Gehen wir aus von einem Complexe mit fünf reellen Paaren

$$1) \quad x_1\,y_1,\ x_2\,y_2,\ x_3\,y_3,\ x_4\,y_4,\ x_5\,y_5,$$

und nehmen zunächst an, dass ausser dem letzten Paare dieses Complexes noch eine imaginäre Doppeltangente ξ existire, dann ist auch eine conjugirte Doppeltangente ξ' vorhanden, und der durch das Paar $\xi\,\xi'$ bestimmte reelle Complex 2) ist mit 1) syzygetisch [weil ξ und ξ' nicht in 1) vorkommen]. Die vier gemeinschaftlichen Elemente von 1) und 2) müssen aber reell

sein, weil 2) als reeller Complex keine reelle Doppeltangente mit einer imaginären gepaart enthalten kann.

Es sei also

$$2) \quad \xi\,\xi', \quad x_1\,x_2, \quad y_1\,y_2,$$

und daraus leiten wir die zwei Complexe her:

$$3) \quad x_1\,\xi, \quad x_2\,\xi'$$
$$4) \quad x_1\,\xi', \quad x_2\,\xi,$$

die mit einander syzygetisch sind, und mithin ausser den vier angegebenen kein Element gemein haben. Sie sind aber zugleich conjugirt, und daher kann in 3) ausser x_1, x_2 keine reelle Doppeltangente vorkommen. Nun sind aber 1) und 3) azygetisch, weil ξ in 1) nicht vorkommt; mithin muss aus jedem Paare von 1) ein Element in 3) vorkommen. Also enthält 3) ausser x_1, x_2 noch reelle Elemente, wodurch sich der Widerspruch ergiebt.

Wir schliessen daraus, dass die beiden Complexe, die durch die Paare $x_1\,x_2$, $y_1\,y_2$ bestimmt sind und mit 1) ein syzygetisches Complextripel ausmachen, nur reelle Elemente enthalten.

Lassen wir einen dieser Complexe, etwa $x_1\,x_2$, an Stelle von 1) treten und wiederholen dann unseren Schluss, so ergiebt sich, dass überhaupt alle Doppeltangenten, also auch die des letzten Paares von 1), reell sein müssen.

5. Wenn mehr als acht reelle Doppeltangenten vorhanden sind, so giebt es sechzehn, die in einem syzygetischen Complextripel je vier reelle Paare bilden.

Nehmen wir mehr als acht reelle Doppeltangenten an, so können wir nach den Sätzen 3., 4. folgendes syzygetische Complextripel zusammenstellen:

$$1) \quad x_1\,y_1, \quad x_2\,y_2, \quad x_3\,y_3, \quad x_4\,y_4$$
$$2) \quad x_1\,x_2, \quad y_1\,y_2, \quad z_1\,z_2$$
$$3) \quad x_1\,y_2, \quad x_2\,y_1,$$

worin die x_i, y_i, z_i reell sind.

Damit verbinden wir den Complex

$$4) \quad x_1\,z_1, \quad x_2\,z_2,$$

der mit 1) azygetisch ist, und daher aus den Paaren $x_3\,y_3$, $x_4\,y_4$ je ein und nur ein Element enthalten kann, etwa x_3 und x_4. Da aber 4) ein reeller Complex ist, so muss es zwei weitere

reelle Doppeltangenten z_3, z_4 geben, so dass der Complex 4) sich so fortsetzt:

$$4)\quad x_1 z_1,\; x_2 z_2,\; x_3 z_3,\; x_4 z_4;$$

z_3 und z_4 kommen nicht in 2) und auch nicht in 1) vor, und müssen also in 3) enthalten sein.

Sie können auch in 3) nicht gepaart vorkommen, weil x_1, z_3, z_4 azygetisch sind. Hieraus schliessen wir, wenn t_3, t_4 zwei weitere reelle Doppeltangenten sind, auf folgende Zusammensetzung des Complexes 3):

$$3)\quad x_1 y_2,\; x_2 y_1,\; z_3 t_3,\; z_4 t_4.$$

Betrachtet man nun an Stelle des Complexes 4) den Complex

$$5)\quad x_1 z_3,\; y_2 t_3,$$

so kann man genau ebenso auf ein viertes reelles Paar $u_1 u_2$ im Complex 2) schliessen, und damit ist 5. bewiesen.

Fassen wir das Ergebniss zusammen, so erkennen wir, dass in Bezug auf die Realität der Doppeltangenten einer reellen Curve vierter Ordnung nur vier Fälle möglich sind:

1) Vier reelle syzygetische Doppeltangenten.
2) Acht reelle Doppeltangenten, und zwar vier Paare eines Steiner'schen Complexes.
3) Sechzehn reelle Doppeltangenten, die in einem syzygetischen Complextripel je vier reelle Paare bilden.
4) Achtundzwanzig reelle Doppeltangenten.

§. 105.

Beweis der Existenz der vier Fälle.

Wir haben im vorigen Paragraphen zunächst nur bewiesen, dass es keine anderen als die Fälle 1), 2), 3), 4) geben kann. Dass diese vier Fälle aber wirklich alle möglich sind, ist jetzt auch leicht zu zeigen, auf Grund des Satzes §. 100, nach dem man aus sieben beliebig gegebenen geraden Linien auf rationalem Wege eine Curve vierter Ordnung ableiten kann, für die die gegebenen Linien ein Aronhold'sches System bilden, aus dem sich alle Doppeltangenten rational ableiten lassen.

Unter den sieben gegebenen geraden Linien können auch imaginäre vorkommen, und als Bedingung der Realität der Curve

(d. h. der Coëfficienten in ihrer Gleichung) ergiebt sich die, dass das System, was man erhält, wenn man jede imaginäre Gerade durch ihre conjugirte ersetzt, wieder ein Aronhold'sches System derselben Curve ist. Denn dann ändern sich die Coëfficienten nicht, wenn i durch $-i$ ersetzt wird.

Die Curve wird also gewiss reell, wenn in dem gegebenen Siebener-Systeme zu jeder imaginären Geraden die conjugirte vorkommt; dann bilden sie ein reelles Siebener-System.

Ein solches reelles System kann nun enthalten:

1) eine reelle, drei Paar conjugirt imaginäre Geraden;
2) drei reelle und zwei Paar conjugirt imaginäre Geraden;
3) fünf reelle und ein Paar conjugirt imaginäre Geraden;
4) sieben reelle Geraden.

Wir werden sehen, dass diese vier Annahmen in derselben Ordnung zu den im vorigen Paragraphen aufgezählten vier Fällen führen.

Dieser Nachweis wird sehr einfach, wenn man sich der Bezeichnungsweise der Doppeltangenten, die wir im §. 99 dargelegt haben, bedient, nach der wir die Steiner'schen Complexe unmittelbar aus der Bezeichnung bilden können.

1) Im ersten Falle bezeichnen wir die gegebenen sieben Geraden mit

$$0,\ 1,\ 1',\ 2,\ 2',\ 3,\ 3',$$

setzen 0 als reell voraus, 1 mit 1', 2 mit 2', 3 mit 3' conjugirt imaginär. Die übrigen 21 Doppeltangenten werden dann durch die Zeichen [0 1], [0 1'], [1 1'], ... bezeichnet.

Nach der Vorschrift des §. 99 erhalten wir die beiden folgenden Steiner'schen Complexe:

(1) 0 [0 1], 1'[1 1'], 2 [1 2], 2'[1 2'], 3 [1 3], 3'[1 3']

(1') 0 [0 1'], 1 [1 1'], 2 [1' 2], 2'[1' 2'], 3 [1' 3], 3'[1' 3'].

Der zu (1) conjugirte Complex muss die Elemente 0, 1, 2, 2', 3, 3' enthalten, und ist also nach §. 98, 7. mit (1') identisch, der diese sechs Elemente gleichfalls enthält.

Daraus folgt, dass [1 1'] reell ist, und dass

[0 1] [0 1']
[1 2] [1' 2']
[1 2'] [1' 2]

conjugirte Paare sind. Da man in dieser Betrachtung 1 mit 2 und 3 vertauschen kann, so folgt, dass 0, [1 1'], [2 2'], [3 3'] reell und alle übrigen Doppeltangenten imaginär sind.

Nach §. 99 können wir leicht einen Steiner'schen Complex bilden, der die vier reellen Doppeltangenten enthält:

0 [1 1'], [2 2'] [3 3'], 1 [0 1'], 1' [0 1], [2 3] [2' 3'], [2 3'] [2' 3],

woraus noch zu sehen ist, dass dieser Complex ausser den reellen Paaren zwei conjugirte Paare und ein conjugirtes Doppelpaar enthält.

Dies ist also der Fall 1) des vorigen Paragraphen.

2) Es seien die sieben gegebenen Geraden:

0, 1, 2, 3, 3', 4, 4',

und darin 0, 1, 2 reell, 3 zu 3' und 4 zu 4' conjugirt. Wir bilden drei Complexe:

(0) 1 [0 1], 2 [0 2], 3 [0 3], 3' [0 3'], 4 [0 4], 4' [0 4']
(3) 0 [0 3], 1 [1 3], 2 [2 3], 3' [3 3'], 4 [3 4], 4' [3 4']
(3') 0 [0 3'], 1 [1 3'], 2 [2 3'], 3 [3 3'], 4 [3' 4], 4' [3' 4'].

Der zu (0) conjugirte Complex enthält 1, 2, 3, 3', 4, 4' und ist folglich mit (0) identisch, d. h. der Complex (0) ist reell. Daraus folgt, dass [0 1], [0 2] reell, [0 3] mit [0 3'] und [0 4] mit [0 4'] conjugirt ist. Ferner ergiebt sich auf die gleiche Weise, dass (3), (3') conjugirte Complexe sind, und dass also [3 3'] reell, [3 4] mit [3' 4'], [3 4'] mit [3' 4] conjugirt imaginär sind. Da man 0, 1, 2 beliebig vertauschen darf, und ebenso 3 mit 4, so erhalten wir folgende Zusammenstellung:

Reelle Doppeltangenten:

0, 1, 2, [1 2], [2 0], [0 1], [3 3'], [4 4'].

Conjugirte Paare:

3	4	[0 3]	[0 4]	[1 3]	[1 4]	[2 3]	[2 4]	[3 4]	[3 4']
3'	4'	[0 3']	[0 4']	[1 3']	[1 4']	[2 3']	[2 4']	[3' 4']	[3' 4].

Der Steiner'sche Complex, der vier reelle Paare enthält, ist hier

0 [1 2], 1 [2 0], 2 [0 1], [3 3'] [4 4'], [3 4] [3' 4'], [3 4'] [3' 4],

und er enthält noch zwei conjugirte Paare. Dies ist also der Fall 2) des §. 104.

3) Es seien die gegebenen Linien:

0, 1, 2, 3, 4, 5, 5',

und davon 0, 1, 2, 3, 4 reell, 5 und 5' conjugirt imaginär. Die Betrachtung der drei Complexe:

(0) 1[10], 2[20], 3[30], 4[40], 5[50], 5'[5'0]
(5) 0[05], 1[15], 2[25], 3[35], 4[45], 5'[5'5]
(5') 0[05'], 1[15'], 2[25'], 3[35'], 4[45'], 5[55'],

von denen der erste reell, die beiden anderen conjugirt imaginär sind, und der durch Vertauschung von 0, 1, 2, 3, 4 aus (0) abgeleiteten giebt, genau wie oben, folgendes Resultat:

Reelle Doppeltangenten:

0, 1, 2, 3, 4, [01], [02], [03]
[04] [12], [13] [14], [23], [24], [34], [55'].

Conjugirte Paare:

5, [05], [15], [25], [35], [45]
5', [05'], [15'], [25'], [35'], [45'],

und wir finden ein syzygetisches Complextripel:

0, 1, [02] [12], [03] [13], [04] [14], [05] [15], [05'] [15']
2, 3, [02] [03], [12] [13], [42] [43], [25] [35], [25'] [35']
[01], [23], [02] [13], [03] [12], 4 [55'], 5 [45'], 5' [45],

von denen jeder Complex noch vier reelle Paare und ein imaginäres Doppelpaar enthält. Solcher Tripel lassen sich aber noch mehrere bilden, da man 0, 1, 2, 3, 4 beliebig vertauschen darf. Dies ist der dritte Fall von §. 104.

4) Dass endlich, wenn wir alle Elemente des gegebenen Siebener-Systemes reell voraussetzen, auch alle übrigen Doppeltangenten reell ausfallen, ist eine unmittelbare Folge der rationalen Darstellung (§. 100).

Hiermit ist gezeigt, dass die vier Fälle des vorigen Paragraphen wirklich alle vorkommen können. Ob die hier besprochene Erzeugungsweise die einzig mögliche ist, mit anderen Worten, ob bei jeder reellen Curve vierter Ordnung ein reelles Aronhold'sches System existirt, diese Frage müssen wir unentschieden lassen.

Auch ist hier noch darauf hinzuweisen, dass aus der Realität einer Doppeltangente noch keineswegs die Realität der Berührungspunkte folgt, weil diese Berührungspunkte wieder von einer quadratischen Gleichung abhängen. Die reellen Doppeltangenten zerfallen also wieder in zwei Arten, solche mit reellen und solche mit imaginären Berührungspunkten. Was hier für mögliche Fälle zu unterscheiden sind, diese Frage erörtern wir nicht weiter [1]).

---

[1]) Vergl. über die ganze Frage von der Realität der Doppeltangenten vom geometrischen Gesichtspunkte: Zeuthen, „Sur les différentes formes des courbes planes du quatrième ordre". Mathem. Ann., Bd. VII (1873).

Dreizehnter Abschnitt.

Allgemeine Theorie der Gleichung fünften Grades.

---

§. 106.

Fragestellung.

Wir haben im §. 44 gesehen, dass es über die Frage nach der Galois'schen Gruppe einer algebraischen Gleichung noch ein weiter gehendes Problem giebt, nämlich die Frage nach der linearen Substitutionsgruppe von möglichst geringer Dimensionenzahl, auf deren Formenproblem die gegebene Gleichung zurückführbar ist. Bei den metacyklischen Gleichungen, insbesondere also auch bei den allgemeinen Gleichungen 3ten und 4ten Grades, ist diese Dimensionenzahl gleich 1, wodurch eben ausgedrückt ist, dass diese Gleichungen durch Radicale lösbar sind. Die zunächst zu untersuchenden Gleichungen sind dann die vom 5ten Grade, und es wird sich zeigen, dass die Lösung der allgemeinen Gleichung 5ten Grades auf eine binäre lineare Substitutionsgruppe, nämlich auf das Ikosaëderproblem führt.

Damit im Zusammenhange steht aber noch eine andere Frage.

Die allgemeine Gleichung 5ten Grades enthält fünf Coëfficienten, die als unabhängige Variable betrachtet werden können, und folglich ist die Wurzel einer solchen Gleichung eine algebraische Function von fünf Variablen. Nun kann man aber schon durch die einfachen linearen Substitutionen die Zahl dieser Variablen vermindern. Durch Tschirnhausen-Transformation, z. B. auf die Jerrard'sche Form, kann man die Gleichung sogar nur von einem variablen Coëfficienten (einem Parameter) abhängig machen, und man kann also, durch Vermittelung von Gleichungen, die den 5ten Grad nicht erreichen, die Wurzel einer allgemeinen Gleichung 5ten Grades von einer algebraischen Function von einer Variablen abhängig machen.

Die Frage, auf die wir hier geführt werden, ist also die, wie man die Lösung einer algebraischen Gleichung, deren Coëfficienten von einer gewissen Anzahl von Variablen abhängen, auf eine Gleichung mit einer möglichst geringen Anzahl von Parametern, und insbesondere, unter welchen Umständen und mit welchem Hülfsmittel man sie auf Gleichungen mit nur einem Parameter zurückführen kann.

Wir stellen uns demnach jetzt die Frage, unter welchen Voraussetzungen bei einer allgemeinen Gleichung n^{ten} Grades Resolventen mit nur einem Parameter existiren.

Es sei $x_0, x_1, \ldots, x_{n-1}$ ein System von n unabhängigen Variablen,

(1) $$u = \Phi(x_0, x_1, \ldots, x_{n-1})$$

eine rationale Function dieser Variablen, die durch die Permutationen der alternirenden Gruppe der n Buchstaben x in die von einander verschiedenen Functionen

(2) $$u, u_1, u_2, \ldots u_{\nu-1}$$

übergeht, worin ν gleich oder kleiner als der Grad der alternirenden Gruppe sein kann, und z eine Function der Variablen x ist, die durch die alternirende Gruppe ungeändert bleibt. Es fragt sich, wann eine rationale Gleichung ν^{ten} Grades in Bezug auf u besteht,

(3) $$F(u, z) = 0,$$

die durch die ν Functionen (2) identisch befriedigt wird? Die Coëfficienten in (3) müssen von den x unabhängig und also reine Zahlen sein. Eine Beschränkung des Rationalitätsbereiches im Gebiete der Zahlen lassen wir einstweilen nicht eintreten.

Die Gleichung (3) ist, wenn $\nu > 1$ ist, eine Resolvente der Gleichung n^{ten} Grades, deren Wurzeln die x sind, die nur von dem einen Parameter z abhängt. Den Fall $\nu = 1$ schliessen wir aus.

§. 107.

Satz von Lüroth.

Es ist zunächst folgender Hülfssatz zu beweisen[1]):

1. Ist $u, u_1, u_2, \ldots, u_{\nu-1}$ ein System rationaler Functionen einer Variablen t, so giebt es eine rationale Function der $u, u_1, \ldots, u_{\nu-1}$:

$$\vartheta = \chi(u, u_1, \ldots, u_{\nu-1})$$

[1]) Lüroth, Mathematische Annalen, Bd. IX.

von der Art, dass $u, u_1, \ldots, u_{\nu-1}$ rational durch ϑ allein ausgedrückt werden können.

Um ihn zu beweisen, setzen wir

$$(1) \qquad u = \frac{\varphi(t)}{\psi(t)}, \quad u_1 = \frac{\varphi_1(t)}{\psi_1(t)}, \ldots, u_{\nu-1} = \frac{\varphi_{\nu-1}(t)}{\psi_{\nu-1}(t)},$$

und verstehen unter $\varphi(t)$, $\psi(t)$ ganze Functionen von t ohne gemeinschaftlichen Theiler; ebenso unter $\varphi_1(t)$, $\psi_1(t)$ u. s. f. Ausserdem dürfen wir noch voraussetzen, dass von den Functionen $u, u_1, \ldots, u_{\nu-1}$ keine eine Constante sei. Wir führen neben der Variablen t eine zweite Variable τ ein und setzen:

$$(2) \qquad v = \frac{\varphi(\tau)}{\psi(\tau)}, \quad v_1 = \frac{\varphi_1(\tau)}{\psi_1(\tau)}, \ldots, v_{\nu-1} = \frac{\varphi_{\nu-1}(\tau)}{\psi_{\nu-1}(\tau)}.$$

Nun bilden wir die ganzen Functionen der beiden Variablen t, τ, deren keine identisch verschwindet:

$$(3) \qquad \begin{aligned} \varphi(t)\,\psi(\tau) - \varphi(\tau)\,\psi(t) &= \Phi(t,\tau) = -\Phi(\tau,t) \\ \varphi_1(t)\,\psi_1(\tau) - \varphi_1(\tau)\,\psi_1(t) &= \Phi_1(t,\tau) = -\Phi_1(\tau,t) \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ \varphi_{\nu-1}(t)\,\psi_{\nu-1}(\tau) - \varphi_{\nu-1}(\tau)\,\psi_{\nu-1}(t) &= \Phi_{\nu-1}(t,\tau) = -\Phi_{\nu-1}(\tau,t). \end{aligned}$$

Betrachten wir sie als Functionen von t, so verschwinden sie alle, wenn $t = \tau$ wird, und sie haben also einen grössten gemeinschaftlichen Theiler, der in Bezug auf t mindestens vom ersten Grade ist, und vom μ^{ten} Grade sein möge:

$$(4) \qquad R = R(t, \tau).$$

Diese Function R ist auch in Bezug auf τ rational, und wenn man sie so einrichtet, dass τ nicht im Nenner und nicht in einem überflüssigen Factor vorkommt, so kann $R(t,\tau)$ bei der Vertauschung von t und τ höchstens sein Vorzeichen ändern. Denn die Functionen (3) sind, auch als Functionen der beiden Variablen t, τ betrachet, durch $R(t, \tau)$, und da sie alternirend sind, durch $R(\tau, t)$ theilbar (Bd. I, §. 51). Es ist also $R(t, \tau)$ durch $R(\tau, t)$ theilbar, und umgekehrt, und folglich unterscheiden sich beide nur durch einen constanten Factor, der $= \pm 1$ sein muss, weil die nochmalige Vertauschung von t mit τ die ursprüngliche Function wieder herstellt.

Es lässt sich noch beweisen, dass keine der Functionen (3) (bei unbestimmtem τ) als Function von t betrachtet, einen Factor

mehrfach enthält, und dass in Folge dessen auch $R(t, \tau)$ durch kein Quadrat theilbar ist. Angenommen nämlich, es hätten

$$\Phi(t,\tau) = \varphi(t)\,\psi(\tau) - \varphi(\tau)\,\psi(t)$$
$$\Phi'(t,\tau) = \varphi'(t)\,\psi(\tau) - \varphi(\tau)\,\psi'(t)$$

als Functionen von t einen gemeinsamen Theiler P, so müsste P auch Theiler von

$$\psi'(t)\,\Phi - \psi(t)\,\Phi' = [\varphi(t)\,\psi'(t) - \psi(t)\,\varphi'(t)]\,\psi(\tau)$$

sein. Es wäre daher P Theiler von $\varphi(t)\,\psi'(t) - \psi(t)\,\varphi'(t)$, und könnte also von τ unabhängig angenommen werden.

Nehmen wir nun zwei Werthe τ_1, τ_2 von τ so an, dass $\Phi(\tau_2, \tau_1)$ von Null verschieden wird, so ist nach (3)

$$\Phi(t,\tau_1)\,\varphi(\tau_2) - \Phi(t,\tau_2)\,\varphi(\tau_1) = \varphi(t)\,\Phi(\tau_2, \tau_1).$$

Darin ist die linke Seite durch P theilbar, und also ist auch $\varphi(t)$ und folglich $\psi(t)$ durch P theilbar, was der Voraussetzung widerspricht, dass diese beiden Functionen ohne gemeinschaftlichen Theiler sein sollen.

Daraus folgt beiläufig, dass $R(t,\tau) = -R(\tau, t)$ sein muss, da R durch $t - \tau$, aber nicht durch $(t - \tau)^2$ theilbar ist.

Um die Function $R(t, \tau)$ zu bilden, kann man den grössten gemeinschaftlichen Theiler der Functionen $\varphi_h(t) - v_h\,\psi_h(t)$ aufsuchen, woraus folgt, dass $R(t, \tau)$, abgesehen von einem von t unabhängigen Factor, rational durch $v, v_1, \ldots, v_{\nu-1}$ dargestellt werden kann. Sind also a und b irgend zwei feste numerische Werthe, so ist

$$(5) \qquad \frac{R(a,\tau)}{R(b,\tau)} = \vartheta = \chi(v, v_1, \ldots, v_{\nu-1})$$

eine rationale Function von $v, v_1, \ldots, v_{\nu-1}$. Dabei ist, wenn ξ eine neue Variable bedeutet:

$$(6) \qquad R(a,\xi) - \vartheta\,R(b,\xi) = X$$

in Bezug auf ξ vom μ^{ten} Grade.

Ist τ ein willkürlicher Werth, so mögen die Wurzeln der Gleichung $R(t,\tau) = 0$

$$(7) \qquad t = \tau, \tau', \tau'', \ldots$$

sein, so dass für jeden Index h

$$\Phi_h(\tau, \tau), \quad \Phi_h(\tau', \tau), \quad \Phi_h(\tau'', \tau), \ldots$$

verschwinden.

Sind τ', τ'' irgend zwei dieser Wurzeln, so folgt aus (3):

$$\varphi_h(\tau')\,\psi_h(\tau) - \varphi_h(\tau)\,\psi_h(\tau') = 0$$
$$\varphi_h(\tau'')\,\psi_h(\tau) - \varphi_h(\tau)\,\psi_h(\tau'') = 0,$$

und daraus, da $\psi_h(\tau)$ und $\varphi_h(\tau)$ nicht zugleich verschwinden können,

$$\varphi_h(\tau')\,\psi_h(\tau'') - \varphi_h(\tau'')\,\psi_h(\tau') = 0,$$

d. h. es ist, wenn τ', τ'' irgend zwei der Grössen (7) sind,

$$\Phi_h(\tau', \tau'') = 0.$$

Daraus folgt, dass die ν Functionen $\Phi_h(t, \tau')$, von einem von t unabhängigen Factor abgesehen, den nämlichen grössten gemeinschaftlichen Theiler haben, wie die Functionen $\Phi_h(t, \tau)$. Das Gleiche gilt für die Functionen $\Phi_h(t, \tau'')$ u. s. f., oder die Gleichungen

$$R(t, \tau) = 0, \quad R(t, \tau') = 0, \quad R(t, \tau'') = 0, \ldots$$

haben alle dieselben Wurzeln. Daraus folgt nach (5):

$$\vartheta = \frac{R(a, \tau)}{R(b, \tau)} = \frac{R(a, \tau')}{R(b, \tau')} = \frac{R(a, \tau'')}{R(b, \tau'')} = \cdots,$$

und mithin sind nach (6) die μ Werthe

$$\xi = \tau, \tau', \tau'', \ldots$$

die Wurzeln der Gleichung $X = 0$. Andererseits folgt aus $\Phi_h(\tau', \tau) = 0$, $\Phi_h(\tau'', \tau) = 0, \ldots$

$$v_h = \frac{\varphi_h(\tau)}{\psi_h(\tau)} = \frac{\varphi_h(\tau')}{\psi_h(\tau')} = \frac{\varphi_h(\tau'')}{\psi_h(\tau'')} \cdots = \frac{1}{\mu} \Sigma \frac{\varphi_h(\tau)}{\psi_h(\tau)},$$

und es kann folglich v_h als symmetrische Function der Wurzeln von (6) rational durch die Coëfficienten dieser Gleichung, d. h. rational durch ϑ dargestellt werden. Vertauscht man wieder t mit τ, so erhält man nach (1) und (2) Ausdrücke von der Form

(10) $$u = f(\vartheta),\ u_1 = f_1(\vartheta), \ldots, u_{\nu-1} = f_{\nu-1}(\vartheta)$$
$$\vartheta = \chi(u, u_1, \ldots, u_{\nu-1}),$$

worin $f, f_1, \ldots, f_{\nu-1}, \chi$ rationale Functionen bedeuten.

§. 108.

Resolventen mit einem Parameter.

Wir kehren jetzt zu unseren anfänglichen Voraussetzungen (§. 106) zurück, und bezeichnen mit $u, u_1, \ldots, u_{\nu-1}$ ein System

rationaler Functionen von $x_0, x_1, \ldots, x_{n-1}$, die durch die Permutationen der alternirenden Gruppe aus einer von ihnen hervorgehen und Wurzeln der Gleichung

$$F(u, z) = 0 \tag{1}$$

sind, worin z eine rationale Function der x ist, die durch die Permutationen der alternirenden Gruppe ungeändert bleibt.

Wir beweisen folgenden zweiten Hülfssatz:

2. Wenn die rationale Function $\Psi(u, u_1, \ldots, u_{\nu-1})$ identisch verschwindet, wenn für die

$$x_0, x_1, \ldots, x_{n-1}$$

gewisse rationale Functionen einer Variablen t

$$x_h = \varphi_h(t) \tag{2}$$

gesetzt werden, und wenn durch diese Substitution z nicht von t unabhängig wird, so verschwindet Ψ identisch auch als Function der unabhängigen Variablen $x_0, x_1, \ldots, x_{\nu-1}$.

Die Galois'sche Gruppe der Gleichung (1) in dem Körper der rationalen Functionen von z wird aus gewissen Permutationen der Wurzeln $u, u_1, \ldots, u_{\nu-1}$ bestehen. Führen wir diese Permutationen in der Function Ψ aus, und bilden das Product

$$\Pi\, \Psi(u, u_1, \ldots, u_{\nu-1}) = f(z) \tag{3}$$

aller so erhaltenen Functionen, so ergiebt sich eine rationale Function $f(z)$ von z. Wenn nun einer der Factoren des Productes (3) nach der Substitution (2) identisch verschwindet, und z ist nicht von t unabhängig, so muss $f(z)$ identisch gleich Null sein, und folglich muss einer der Factoren des Productes (3) auch als Function der x identisch verschwinden. Wenn aber einer dieser Factoren identisch gleich Null ist, so verschwinden auch alle anderen Factoren, weil man in jeder rationalen Gleichung zwischen den u alle Permutationen der Galois'schen Gruppe ausführen kann. Damit ist der Satz 2. bewiesen.

Dieser Satz giebt nun mit dem im vorigen Paragraphen bewiesenen Satze 1. zusammengenommen das folgende Resultat:

3. Sind $u, u_1, \ldots, u_{\nu-1}$ die Wurzeln einer von einem Parameter z abhängigen Gleichung (1), und sind $u, u_1, \ldots, u_{\nu-1}, z$ rationale Functionen der

unabhängigen Variablen $x_0, x_1, \ldots, x_{n-1}$, so kann man

(4) $$u = f(\vartheta),\ u_1 = f_1(\vartheta), \ldots, u_{\nu-1} = f_{\nu-1}(\vartheta)$$

setzen, worin $f, f_1, \ldots, f_{\nu-1}$ rationale Functionen von ϑ sind und

(5) $$\vartheta = \chi(u, u_1, \ldots, u_{\nu-1}) = \psi(x_0, x_1, \ldots, x_{n-1})$$

eine rationale Function der u, oder auch der x ist.

Nach dem Satze 1. nämlich können wir zunächst, wenn wir $x_0, x_1, \ldots, x_{n-1}$ durch rationale Functionen einer Variablen t ersetzen, so dass z nicht von t unabhängig wird, die Functionen u_h durch die Formeln (4), (5) darstellen. Die Relationen

$$u_h = f_h(\vartheta) = f_h[\chi(u, u_1, \ldots, u_{\nu-1})]$$

sind dann in Bezug auf t identisch befriedigt, und müssen also nach dem Satze 2. auch in den Variablen x identisch sein, w. z. b. w.

4. Wenn von zwei Variablen ϑ, ϑ_1 jede eine rationale Function der anderen ist, so sind sie lineare Functionen von einander.

Zum Beweise nehmen wir an, es sei

(6) $$\vartheta = \frac{\varphi(\vartheta_1)}{\psi(\vartheta_1)},\quad \vartheta_1 = \frac{\varphi_1(\vartheta)}{\psi_1(\vartheta)},$$

und verstehen unter φ, ψ zwei ganze Functionen ohne gemeinsamen Theiler, ebenso unter φ_1, ψ_1. Ordnen wir die zweite der Gleichungen (6) in der Form $\varphi_1(\vartheta) - \vartheta_1 \psi_1(\vartheta) = 0$ nach Potenzen von ϑ, so mag sie die Gestalt annehmen:

$$a_0 \vartheta^m + a_1 \vartheta^{m-1} + \cdots + a_{m-1} \vartheta + a_m = 0,$$

worin die Coëfficienten $a_0, a_1, \ldots, a_m$ ganze lineare Functionen von ϑ_1 sind. Substituiren wir darin für ϑ den Werth aus der ersten Gleichung (6), so folgt die in Bezug auf ϑ_1 identische Gleichung

$$a_0 \varphi^m + a_1 \varphi^{m-1} \psi + \cdots + a_{m-1} \varphi \psi^{m-1} + a_m \psi^m = 0.$$

Hiernach muss $a_0 \varphi^m$ durch ψ theilbar sein, und weil φ und ψ relativ prim vorausgesetzt sind, so muss a_0 durch ψ theilbar, also ψ constant oder linear sein. Ebenso schliessen wir, dass φ constant oder linear sein muss, und da nicht beide

Functionen constant sein können, so ist nach (6) der Satz 4. bewiesen.

Diesen Satz wenden wir auf die in 3. vorkommende Function ϑ an. Wenn wir mit den Variablen x irgend eine Permutation der alternirenden Gruppe vornehmen, so erfahren die Functionen $u, u_1, \ldots, u_{\nu-1}$ gleichfalls eine Permutation. Nach (5) geht ϑ durch diese Permutation in eine andere Function ϑ_1 über, die nach (4) rational durch ϑ darstellbar ist. Ebenso ist aber auch ϑ rational durch ϑ_1 darstellbar, da man in dem Satze 3. ϑ durch ϑ_1 ersetzen kann, und auch ϑ aus ϑ_1 durch eine Permutation der alternirenden Gruppe entsteht. Es sind also nach 4. ϑ und ϑ_1 lineare Functionen von einander. Daraus ergiebt sich das folgende Resultat:

5. Wenn bei einer allgemeinen Gleichung n^{ten} Grades eine Resolvente mit einem Parameter besteht, so giebt es eine rationale Function ϑ von n Variablen x, die durch die Permutationen der alternirenden Gruppe in eine lineare Function von sich selbst

$$\chi(\vartheta) = \frac{a\vartheta + b}{c\vartheta + d} \tag{7}$$

übergeht, worin a, b, c, d Constante, d. h. Zahlen sind.

§. 109.

Gruppe der Resolventen mit einem Parameter.

Die Function ϑ, die im Satze 5. des vorigen Paragraphen vorkommt, ist nach dem Satze 3. selbst die Wurzel einer Resolvente mit einem Parameter $\Phi(\vartheta, z) = 0$. Diese Gleichung ist, da jede Wurzel rational durch jede andere ausdrückbar ist, eine Normalgleichung, und ihre Galois'sche Gruppe ist isomorph mit der Gruppe der linearen Substitutionen $\chi(\vartheta)$ des Satzes 5. Da man nun in der identischen Gleichung $\Phi(\vartheta, z) = 0$ alle Permutationen der alternirenden Gruppe A der Variablen x ausführen kann, wodurch sich z nicht ändert, während ϑ in jede andere Wurzel von Φ übergeht, so ist die Gruppe der linearen Substitutionen $\chi(\vartheta)$, d. h. die Galois'sche Gruppe der Glei-

chung Φ, mit der alternirenden Permutationsgruppe von n Ziffern (ein- oder mehrstufig) isomorph. Die Gruppe der linearen Substitutionen $\chi(\vartheta)$ möge mit L bezeichnet sein. Sie muss, da sie endlich ist, mit einer der im siebenten Abschnitte betrachteten Polyëdergruppen identisch sein.

Zur Vereinfachung machen wir nun von dem in §. 51, 2. bewiesenen Satze Gebrauch, nach dem sich die Gruppe L so transformiren lässt, dass eine beliebige der nicht identischen Substitutionen von L eine Multiplication wird. Eine Transformation der Gruppe L ist aber gleichbedeutend damit, dass für ϑ eine lineare Function von ϑ gesetzt wird, der dieselbe Eigenschaft wie der ursprünglichen Function ϑ zukommt.

Bezeichnen wir also mit ϑ_π die Function der Variablen $x_0, x_1, \ldots, x_{n-1}$, die aus ϑ durch Anwendung der Permutation π hervorgeht, so können wir ϑ so wählen, dass für eine bestimmte, aber beliebige Permutation π

$$\vartheta_\pi = \varepsilon \vartheta$$

wird. Wendet man π wiederholt an, so folgt

$$\vartheta_{\pi^2} = \varepsilon^2 \vartheta, \quad \vartheta_{\pi^3} = \varepsilon^3 \vartheta, \ldots,$$

und wenn also p der Grad der Permutation π ist, so ist ε eine p^{te} Einheitswurzel.

Ist zunächst $n = 3$, so besteht die alternirende Gruppe aus den Potenzen der cyklischen Permutation $\gamma = (0, 1, 2)$. Wir können annehmen, dass die der Permutation entsprechende Substitution $\chi(\vartheta)$ multiplicativ sei, dass also $\vartheta_\gamma = \varepsilon \vartheta$ sei, worin ε eine dritte Einheitswurzel ist. ϑ^3 ist daher eine alternirende (oder symmetrische) Function. Als Resolvente mit einem Parameter erhalten wir also die reine Gleichung

$$\vartheta^3 = z,$$

wo z eine alternirende Function ist. Wir können etwa für ϑ die Lagrange'sche Resolvente $x_0 + \varepsilon x_1 + \varepsilon^2 x_2$ nehmen, und erhalten die bekannte Reduction der cubischen Gleichung auf eine reine Gleichung (Bd. I, §. 159).

Wir gehen zu dem Falle $n = 4$ über, in dem die alternirende Gruppe A die Permutationen

$$1, \ \alpha_1 = (0,1)\,(2,3), \ \alpha_2 = (0,2)\,(1,3), \ \alpha_3 = (0,3)\,(1,2)$$

enthält, die eine Vierergruppe B bilden; ausserdem kommen

in A noch acht cyklische Permutationen von je drei Ziffern $\gamma = (0, 1, 2) \ldots$ vor, und A kann so dargestellt werden:

$$A = B + B\gamma + B\gamma^2.$$

Je eine Permutation α und eine Permutation γ können als Erzeugende der Gruppe betrachtet werden. Denn ist etwa

$$\gamma = (0, 1, 2), \quad \alpha_1 = (0, 1)\,(2, 3),$$

so ist

(1) $$\alpha_1 \gamma \alpha_1 = \gamma' = (0, 3, 1),$$

und aus (0, 1, 2), (0, 3, 1) kann die ganze Gruppe A abgeleitet werden (Bd. I, §. 153, 7.).

Ebenso kann man γ und γ' als erzeugende Permutationen von A auffassen. Insbesondere ist

(2) $$\gamma' \gamma \gamma' = \alpha_1.$$

Wir wählen ϑ so, dass der Permutation γ eine Multiplication $\varepsilon \vartheta$ entspricht, in der, da γ vom Grade 3 ist, ε eine dritte Einheitswurzel bedeutet. Wir setzen

(3) $$\vartheta = \frac{\varphi\,(x_0, x_1, x_2, x_3)}{\psi\,(x_0, x_1, x_2, x_3)},$$

und verstehen unter φ, ψ zwei ganze Functionen der vier Variablen x ohne gemeinschaftlichen Theiler.

Aus der identischen Gleichung

$$\frac{\varphi_\gamma}{\psi_\gamma} = \varepsilon \frac{\varphi}{\psi}$$

folgt dann, dass

(4) $$\varphi_\gamma = \varepsilon_1 \varphi, \quad \psi_\gamma = \varepsilon_2 \varphi$$

sein muss, worin ε_1, ε_2 gleichfalls dritte Einheitswurzeln sind.

Wir wenden eine der Permutationen α auf ϑ an, und erhalten aus $\vartheta_\alpha = \chi(\vartheta)$:

(5) $$\frac{\varphi_\alpha}{\psi_\alpha} = \frac{a\varphi + b\psi}{c\varphi + d\psi}.$$

Da nun φ, ψ, also auch $a\varphi + b\psi$ und $c\varphi + d\psi$, und ebenso φ_α, ψ_α ohne gemeinsamen Theiler sind, so muss in der Identität (5) der Zähler dem Zähler und der Nenner dem Nenner, wenigstens bis auf einen constanten Factor, gleich sein. Diesen constanten Factor können wir in die Constanten a, b, c, d einrechnen und erhalten

6) $$\varphi_\alpha = a\varphi + b\psi, \quad \psi_\alpha = c\varphi + d\psi.$$

Nehmen wir hierin $\alpha = \alpha_1$ und $\alpha = \alpha_2$ an, und setzen zur Abkürzung $\varphi_{\alpha_1} = \varphi_1$, $\varphi_{\alpha_2} = \varphi_2$, so können wir aus den beiden Gleichungen

$$\varphi_1 = a_1 \varphi + b_1 \psi, \quad \varphi_2 = a_2 \varphi + b_2 \psi$$

ψ eliminiren und erhalten eine Gleichung von der Form:

$$h \varphi + h_1 \varphi_1 + h_2 \varphi_2 = 0, \tag{7}$$

worin h, h_1, h_2 Constanten sind, unter denen wenigstens zwei von Null verschieden sind. Auf die identische Gleichung (7) können wir nun die Permutationen α_1, α_2 anwenden, und erhalten, da $\alpha_1 \alpha_2 = \alpha_2 \alpha_1 = \alpha_3$, $\alpha_1 \alpha_1 = 1$, $\alpha_2 \alpha_2 = 1$ ist,

$$\begin{array}{l|l} h\varphi + h_1 \varphi_1 + h_2 \varphi_2 = 0 & h, \\ h\varphi_1 + h_1 \varphi + h_2 \varphi_3 = 0 & h_1, \\ h\varphi_2 + h_1 \varphi_3 + h_2 \varphi = 0 & -h_2, \end{array}$$

woraus durch Multiplication mit den daneben stehenden Factoren und Addition:

$$(h^2 + h_1^2 - h_2^2)\, \varphi + 2\, h h_1 \varphi_1 = 0. \tag{8}$$

Wenn also h und h_1 von Null verschieden sind, so unterscheiden sich φ und φ_1 nur durch einen constanten Factor (der $= \pm 1$ sein muss, da α_1 vom 2ten Grade ist). Ist aber h oder $h_1 = 0$, so folgt aus (7) $\varphi_1 = \pm \varphi_2$ oder $\varphi = \pm \varphi_2$, und die Anwendung von α_1 auf die erste Gleichung giebt $\varphi = \pm \varphi_3$. Es findet also jedenfalls eine der Relationen statt:

$$\varphi = \pm \varphi_1, \quad \varphi = \pm \varphi_2, \quad \varphi = \pm \varphi_3. \tag{9}$$

Da man nun ebensowohl γ, α_1 als γ, α_2, als auch γ, α_3 als erzeugende Elemente der Gruppe A betrachten kann, so ergiebt dies Resultat, zusammengenommen mit (4), den Satz:

1. Die Function φ hat die Eigenschaft, sich durch alle Permutationen der alternirenden Gruppe nur um einen constanten Factor zu ändern.

Ganz derselbe Schluss ist aber auch auf ψ anwendbar, und also auch auf den Quotienten ϑ beider Functionen. Es ist sonach für jede Permutation π der alternirenden Gruppe

$$\vartheta_\pi = \varepsilon\, \vartheta. \tag{10}$$

Hierin ist, wenn π zu den cyklischen Permutationen γ gehört, ε eine dritte Einheitswurzel. Daraus ist aber ferner zu schliessen, weil alle Permutationen π aus γ, γ' zusammengesetzt

werden können, dass die in (10) vorkommende Constante ε immer eine dritte Einheitswurzel ist. Wenn π zu den α gehört, so ist ε zugleich eine zweite Einheitswurzel und muss also $= 1$ sein. Daraus folgern wir den Satz:

2. Die Function ϑ bleibt bei den Permutationen der Vierergruppe A ungeändert.

Die dritte Potenz von ϑ gestattet die Permutationen der alternirenden Gruppe und ϑ ist daher die Wurzel einer reinen cubischen Gleichung $\vartheta^3 = z$. Dies ist also die Resolvente $\Phi(\vartheta, z) = 0$, die in diesem Falle eine Partialresolvente ist (Bd. I, §. 161).

Aus diesen Betrachtungen ergiebt sich nun ohne Schwierigkeit der folgende Satz, dessen Beweis das Ziel dieser ganzen Betrachtungen ist:

3. Eine allgemeine Gleichung von höherem als 4ten Grade hat keine Resolventen mit einem Parameter.

Denn ist n grösser als 4, so können wir, wenn wir ϑ als Function von je vieren der Variablen x betrachten, den Satz 2. anwenden. Es folgt dann, dass ϑ ungeändert bleibt, wenn unter den Variablen irgend ein Paar von Transpositionen vorgenommen wird. Da man nun aus Transpositionspaaren die ganze alternirende Gruppe zusammensetzen kann (Bd. I, §. 153, 8.), so folgt, dass ϑ überhaupt durch die alternirende Gruppe ungeändert bleibt, also eine alternirende oder eine symmetrische Function ist. $\Phi(\vartheta, z) = 0$ reducirt sich auf die Identität $\vartheta = z$ und ist keine Resolvente.

Es sei noch bemerkt, dass, wenn man an Stelle der alternirenden Gruppe die symmetrische treten lässt, dieser Satz a fortiori gilt.

Den Satz, dessen Beweis wir hier entwickelt haben, hat zuerst Kronecker ausgesprochen, ohne einen Beweis dafür zu veröffentlichen. Der erste Beweis ist von F. Klein gegeben, der dann von Gordan noch vereinfacht ist [1]).

---

[1]) F. Klein, Vorlesungen über das Ikosaëder. Der Beweis von Gordan, dem unsere Darstellung in den Grundzügen folgt, findet sich in Bd. 29 der mathematischen Annalen (1887).

§. 110.

Die Ikosaëdergleichung.

Das Resultat dieser Betrachtungen ist zunächst, sofern es die allgemeinen Gleichungen von höherem als dem 4ten Grade betrifft, ein negatives. Es gelingt nicht, durch rationale Resolventenbildung die allgemeine Gleichung 5ten Grades auf eine Gleichung mit einem Parameter zu reduciren. Wollen wir gleichwohl dies Ziel noch nicht aufgeben, so bleibt nichts übrig, als dass wir die Variablen $x_0, x_1, \ldots, x_{n-1}$ nicht mehr als völlig unabhängige Variable auffassen, dass wir zwischen ihnen gewisse Gleichungen bestehen lassen. Wir haben es freilich dann nicht mehr mit der allgemeinen Gleichung des betreffenden Grades zu thun, sondern mit einer specielleren, bei der die Coëfficienten nicht unabhängig von einander sind, und es stellt sich die zweite Frage ein, wie und durch welche irrationale Functionen sich die allgemeine Gleichung auf diese specielle zurückführen lässt. Gelingt dies durch Gleichungen niedrigeren Grades, z. B. durch Quadratwurzeln, so wird immerhin eine Reduction des Problems erreicht sein.

Wir nehmen also jetzt an, dass die Variablen $x_0, x_1, \ldots, x_{n-1}$ durch eine beliebige Anzahl von Relationen

(1) $A\,(x_0, x_1, \ldots, x_{n-1}) = 0, \quad B\,(x_0, x_1, \ldots, x_{n-1}) = 0, \ldots$

mit einander verknüpft seien, worin die $A, B, \ldots$ rationale Functionen der x sind, die an Anzahl und gegenseitiger Abhängigkeit so beschaffen sind, dass die Werthe der x nicht numerisch festgelegt, sondern noch variabel sind. Ausserdem legen wir eine Permutationsgruppe $\mathfrak{A}$ der $x_0, x_1, \ldots, x_{n-1}$ zu Grunde, und betrachten die Functionen der x, die die Permutationen von $\mathfrak{A}$ gestatten, und nur diese als rational, so dass $\mathfrak{A}$ die Galois'sche Gruppe der Gleichung ist, deren Wurzeln die $x_0, x_1, \ldots, x_{n-1}$ sind. Die Relationen (1) müssen dann so beschaffen sein, dass auch sie die Permutationen $\mathfrak{A}$ gestatten.

Wir fragen unter diesen Voraussetzungen nach der Möglichkeit, zwei rationale Functionen u, z von $x_0, x_1, \ldots, x_{n-1}$ so zu bestimmen, dass zwischen ihnen eine Gleichung

(2) $$F\,(u, z) = 0$$

besteht, die für alle den Relationen (1) genügenden Werthe der x befriedigt ist und worin z, immer mit Rücksicht auf die Relationen (1), ungeändert bleibt, wenn die x den Permutationen der Gruppe $\mathfrak{A}$ unterworfen werden. Die Function u soll dadurch in ν verschiedene Functionen

(3) $$u, u_1, \ldots, u_{\nu-1}$$

übergehen, so dass die Grössen (3) die Wurzeln der Gleichung (2) sind, und wenn $\nu > 1$ ist, (2) eine Resolvente der Gleichung für die x ist.

In dieser Allgemeinheit haben wir für die Lösung der Frage bis jetzt noch keinen Angriffspunkt. Wir fügen daher eine weitere beschränkende Voraussetzung hinzu, nämlich: Es soll möglich sein, für die x_h rationale Functionen einer Variablen t

(4) $$x_h = \varphi_h(t)$$

zu setzen, so dass die Relationen (1) identisch befriedigt sind, und dass zugleich z nicht von t unabhängig wird[1]).

Um gleich hier ein Beispiel anzuführen, mit dem wir uns später noch eingehend beschäftigen werden, erwähnen wir den Fall von fünf Variablen x_0, x_1, x_2, x_3, x_4, die den Bedingungen

(5) $$\Sigma x = 0, \quad \Sigma x^2 = 0$$

genügen, und die also die Wurzeln einer Hauptgleichung 5ten Grades sind (Bd. I, §. 54). Dass die Voraussetzung, die wir gemacht haben, in diesem Falle zutrifft, zeigt die Darstellung in Bd. I, §. 74, (4):

$$y = t_3 F_0 + t_2 (\alpha_2 F_1 + \alpha_1 F_2 + \alpha_0 F_3),$$

was, wenn die dort angeführten Bestimmungen getroffen sind für die x gesetzt, den Bedingungen (5) für alle Werthe des Verhältnisses $t = t_2 : t_3$ genügt.

---

[1]) Betrachtet man die x und die u als Coordinaten je eines Punktes X und U in einem Raume von n und ν Dimensionen, so bestimmen die Relationen (1) für x eine Mannigfaltigkeit von weniger als n Dimensionen. Jedem Punkte X entspricht ein Punkt U, und der Gesammtheit der X nach (2) eine Mannigfaltigkeit der U von einer Dimension (einer Curve). Unsere Voraussetzung ist die, dass dies eine sogenannte rationale oder unicursale Curve oder (in der Sprache der Functionentheorie) eine Curve vom Geschlecht Null sei.

Auch wie die allgemeine Gleichung 5ten Grades auf eine diesen Voraussetzungen entsprechende transformirt werden kann, ist dort gezeigt.

Unter der Voraussetzung (4) hat das Bestehen der Relationen (1) keinen Einfluss auf die Schlüsse des §. 108, und wir haben dann die folgenden Sätze.

Es sei $x_0, x_1, \ldots, x_{n-1}$ ein System von Variablen, das den Relationen $A = 0$, $B = 0, \ldots$ unterworfen, aber sonst unabhängig ist, und es sei $\mathfrak{A}$ eine Permutationsgruppe der x, deren Permutationen die Functionen $A, B, \ldots$ ungeändert lassen.

Soll die Gleichung, deren Wurzeln die Grössen x sind, eine Resolvente

$$F(u, z) = 0 \tag{6}$$

besitzen, die ausser numerischen Coëfficienten nur einen Parameter enthält, der eine durch die Gruppe $\mathfrak{A}$ ungeänderte Function der x ist, so muss eine Function ϑ der Variablen $x_0, \ldots, x_{n-1}$ existiren, die durch die Permutationen α von $\mathfrak{A}$ (mit Rücksicht auf die Relationen $A = 0$, $B = 0, \ldots$) lineare Substitutionen erleidet

$$\vartheta_\alpha = \frac{a\vartheta + b}{c\vartheta + d}, \tag{7}$$

worin a, b, c, d numerische Coëfficienten sind. Die Wurzeln der Gleichung (6) sind rational durch ϑ ausdrückbar, und folglich ist auch ϑ Wurzel einer Gleichung mit einem Parameter

$$\Phi(\vartheta, z) = 0. \tag{8}$$

Ist (6) eine Totalresolvente, was immer eintritt, wenn die Gruppe $\mathfrak{A}$ einfach ist, so können auch die x rational durch ϑ und die zur Gruppe $\mathfrak{A}$ gehörigen Functionen ausgedrückt werden.

Bis hierher findet also vollständige Uebereinstimmung mit den Resultaten des §. 108 statt.

Die Beschränkung aber, auf die wir im §. 109 gestossen sind, wird hier nicht mehr nothwendig eintreten, weil jetzt nicht mehr, wie im Falle völlig unabhängiger Variablen, aus der Gleichheit zweier gebrochener Functionen auf die Uebereinstimmung von Zähler und Nenner geschlossen werden kann.

Die linearen Substitutionen (7) bilden eine mit $\mathfrak{A}$ (ein- oder mehrstufig) isomorphe Gruppe P, die mit einer unserer

Polyëdergruppen identisch sein muss. Wir wollen hier nur den interessantesten Fall eingehender behandeln, dass P die **Ikosaëdergruppe** ist, die wir überdies ohne Beschränkung der Allgemeinheit in der Normalform (§. 58) annehmen können.

Für diese Gruppe haben wir in §. 60 die drei Grundformen abgeleitet. Bezeichnen wir die Variablen dieser Grundformen mit y_1, y_2, so sind es die drei homogenen Functionen 12ten, 20sten und 30sten Grades:

$$
(9)\quad
\begin{aligned}
f(y) &= y_1 y_2 (y_1^{10} + 11\, y_1^5 y_2^5 - y_2^{10})\\
H(y) &= -\, y_1^{20} - y_2^{20} + 228\, (y_1^{15} y_2^5 - y_2^{15} y_1^5) - 494\, y_1^{10} y_2^{10}\\
T(y) &= y_1^{30} + y_2^{30} + 522\, (y_1^{25} y_2^5 - y_1^5 y_2^{25})\\
&\qquad - 10005\, (y_1^{20} y_2^{10} + y_2^{20} y_1^{10}),
\end{aligned}
$$

zwischen denen noch die Relation

$$
(10)\qquad T^2 + H^3 = 1728\, f^5
$$

besteht.

Wenn wir in dem Quotienten $T^2 : f^5$ für das Verhältniss $y_1 : y_2$ einen der 60 Werthe ϑ_α setzen, die aus ϑ durch die Ikosaëdersubstitutionen entstehen, so erhält dieser Quotient immer denselben Werth, der sich also rational durch die Coëfficienten der Gleichung (8), d. h. rational durch z ausdrücken lässt. Wir können ihn geradezu gleich z setzen, und erhalten für die Resolvente (8) die Form

$$
(11)\qquad T^2 - z f^5 = 0,
$$

was wegen (10) mit

$$
H^3 - (1728 - z) f^5 = 0
$$

gleichbedeutend ist. Diese Gleichung ist in Bezug auf y_1, y_2 homogen und vom 60sten Grade, und wenn wir $y_2 = 1$ setzen, so sind ihre 60 Wurzeln $y_1 = \vartheta_\alpha$. Es ist die **Ikosaëdergleichung**, die schon im §. 60 definirt war, und die also ausführlich, in der Form (11) geschrieben, so lautet:

$$
\begin{aligned}
(\vartheta^{30} + 522\, \vartheta^{25} - 10005\, \vartheta^{20} - 10005\, \vartheta^{10} - 522\, \vartheta^5 + 1)^2&\\
= z\, \vartheta^5 (\vartheta^{10} + 11\, \vartheta^5 - 1)^5.&
\end{aligned}
$$

Das Problem, wie wir es also jetzt gefasst haben, kommt auf die Frage hinaus:

Welche Gleichungen lassen sich durch die Ikosaëdergleichung lösen?

§. 111.

Die Resolventen der Ikosaëdergleichung.

Die Formulirung des Problems, die wir am Schluss des vorigen Paragraphen gegeben haben, führt uns auf die Frage nach den verschiedenen Resolventen der Ikosaëdergleichung. Jedem Theiler der Ikosaëdergruppe entspricht eine solche Resolvente, deren Grad gleich dem Index des Theilers, also immer ein Theiler von 60 ist. Nun enthält die Ikosaëdergruppe (§. 59):

1) Tetraëdergruppen (§. 56):	Resolventen	5ten	Grades
2) Diëdergruppen D_5 (§. 55):	"	6ten	"
3) Diëdergruppen D_3:	"	10ten	"
4) Cyklische Gruppen C_5:	"	12ten	"
5) Vierergruppen D_2:	"	15ten	"
6) Cyklische Gruppen C_3:	"	20sten	"
7) Cyklische Gruppen C_2:	"	30sten	"

Da die Ikosaëdergruppe einfach ist, sind alle diese Gleichungen Totalresolventen von einander; wir beschränken uns hier auf die Betrachtung der wichtigsten unter ihnen.

Die Resolventen niedrigsten, nämlich 5ten Grades sind die zu der Tetraëdergruppe gehörigen.

Um sie zu finden, müssen wir eine Function von ϑ suchen, die durch die Substitutionen der Tetraëdergruppe ungeändert bleibt, während sie in der Ikosaëdergruppe fünfwerthig ist.

Wir nehmen die Ikosaëdergruppe in der in §. 58, (22) aufgestellten Normalform, und nehmen die darin enthaltene Tetraëdergruppe Q (§. 59) heraus, die wir über der Vierergruppe

(1) $$1,\ \psi,\ \chi,\ \psi\chi$$

construirt haben, worin, wenn ε eine imaginäre fünfte Einheitswurzel ist, ψ und χ die Bedeutung haben:

(2) $$\psi(x) = \frac{-1}{x},\ \chi(x) = \frac{\omega x + 1}{x - \omega},\ \omega = \varepsilon + \varepsilon^{-1}.$$

Setzen wir $\Theta(x) = \varepsilon x$, so wird die ganze Ikosaëdergruppe

(3) $$P = Q + Q\Theta + Q\Theta^2 + Q\Theta^3 + Q\Theta^4,$$

und

(4) $$Q_h = \Theta^{-h}\, Q\, \Theta^h$$

sind die zu Q conjugirten Tetraëdergruppen.

Nun haben wir im §. 56 zwei Formen f und H vom 6ten und 8ten Grade kennen gelernt, die durch die Tetraëdersubstitutionen, wenn sie homogen und mit der Determinante 1 genommen werden, absolut ungeändert bleiben. Diese Formen können wir freilich nicht geradezu in der Form anwenden, wie sie dort gegeben sind, weil dort die Tetraëdergruppe in anderer Gestalt vorausgesetzt war. Wir finden aber die erste dieser Formen sehr einfach, wenn wir uns erinnern, dass ihre Wurzeln die zweizähligen Pole der Tetraëdergruppe waren, also die Wurzeln der drei Gleichungen

$$x = \psi(x), \quad x = \chi(x), \quad x = \psi\chi(x)$$

oder

$$x^2 + 1 = 0, \quad x^2 - 2\omega x - 1 = 0, \quad \omega x^2 + 2x - \omega = 0,$$

und man erhält also mit Benutzung der Relation

$$\omega^2 + \omega = 1$$

die Gleichung für die zweizähligen Pole

$$(x^2 + 1)(x^4 + 2x^3 - 6x^2 - 2x + 1) = 0.$$

Daher wird die gesuchte Tetraëderform 6ten Grades in den homogenen Variablen x_1, x_2

$$(5) \quad t(x_1, x_2) = x_1^6 + 2x_1^5 x_2 - 5x_1^4 x_2^2 - 5x_1^2 x_2^4 - 2x_1 x_2^5 + x_2^6.$$

Die zweite Tetraëderform, die wir suchen, ist die Hesse'sche Determinante hiervon.

Setzen wir

$$\tilde{\omega}(x_1, x_2) = \frac{1}{5^2 . 4^2} \{t''(x_1, x_1)\, t''(x_2, x_2) - [t''(x_1, x_2)]^2\},$$

so ergiebt eine einfache Rechnung

$$(6) \quad \tilde{\omega}(x_1, x_2) = -(x_1^8 + x_2^8) + (x_1^7 x_2 - x_1 x_2^7) - 7(x_1^6 x_2^2 + x_1^2 x_2^6) - 7(x_1^5 x_2^3 - x_1^3 x_2^5).$$

Wir führen noch die drei Ikosaëderformen 12ten, 20sten und 30sten Grades an, die ja auch durch die Tetraëdersubstitutionen ungeändert bleiben (§. 60):

$$(7) \quad f(x_1, x_2) = x_1 x_2 (x_1^{10} + 11 x_1^5 x_2^5 - x_2^{10})$$

$$(8) \quad H(x_1, x_2) = -(x_1^{20} + x_2^{20}) + 228(x_1^{15} x_2^5 - x_1^5 x_2^{15}) - 494 x_1^{10} x_2^{10}$$

$$(9) \quad T(x_1, x_2) = (x_1^{30} + x_2^{30}) + 522(x_1^{25} x_2^5 - x_1^5 x_2^{25}) - 10005(x_1^{20} x_2^{10} + x_2^{20} x_1^{10}).$$

Bilden wir aus diesen invarianten Formen des Tetraëders Functionen von $x_1 : x_2$ und setzen $\vartheta = x_1 : x_2$, so ergeben sich Functionen, die durch die linearen gebrochenen Tetraëdersubstitutionen ungeändert bleiben, und die daher Wurzeln von Resolventen 5ten Grades der Ikosaëdergleichung sind. Die Ikosaëdergleichung selbst erhält man in zwei Formen, wenn man

(10) $$H^3 = z f^5, \quad T^2 = z_1 f^5, \quad z + z_1 = 1728$$

setzt, und die Resolventen hängen rational von z ab.

Bezeichnen wir für den Augenblick mit $\varphi(x_1, x_2)$ irgend eine absolut invariante Form des Tetraëders, so geht diese Form durch irgend eine der Substitutionen $Q\Theta$ in

(11) $$\varphi_\varepsilon = \varphi(\varepsilon^{-2} x_1, \varepsilon^2 x_2)$$

über, und diese Function bleibt ungeändert durch die Substitutionen der Gruppe $\Theta^{-1} Q \Theta$.

Daraus ergiebt sich, dass jede symmetrische Function der fünf Formen φ_ε eine Invariante der Ikosaëdergruppe ist, und daher nach dem Satze §. 61 durch die Grundformen f, H, T ausgedrückt werden kann.

Dieser Satz gestattet eine verhältnissmässig leichte Berechnung der Resolventen.

Die einfachsten Functionen, die wir als Wurzeln von Resolventen verwenden können, sind

(12) $$r = \frac{t^2}{f}, \quad u = \frac{f^2 t}{T}, \quad v = \frac{f \tilde{\omega}}{H}.$$

Bemerken wir zunächst, dass die symmetrischen Grundfunctionen der fünf Functionen t_ε Ikosaëderinvarianten der Grade 6, 12, 18, 30 sind, so folgt aus den Sätzen in §. 61, da die Gradzahlen 6, 18 unter diesen Invarianten nicht vorkommen, eine Gleichung von der Form

(13) $$t^5 + a f t^3 + b f^2 t + c T = 0,$$

worin a, b, c Zahlencoëfficienten sind. Um sie zu bestimmen, bezeichnen wir mit $S(\varphi)$ die Summe der fünf Functionen φ_ε in (11) und mit $\Pi(\varphi)$ ihr Product, und erhalten aus den Newton'schen Formeln (Bd. I, §. 42):

(14) $$a f = -\tfrac{1}{2} S(t^2), \quad b f^2 = \tfrac{1}{2} a^2 f^2 - \tfrac{1}{4} S(t^4), \quad c T = -\Pi(t).$$

In den Summen $S(\varphi)$ haben nur solche Glieder $x_1^h x_2^k$ einen von Null verschiedenen Coëfficienten, in denen $h - k$ durch 5 theilbar ist. Man erhält also a, b, c durch Gleichsetzen der

Coëfficienten von $x_1^{11} x_2$, $x_1^{22} x_2^2$, x_1^{30} auf beiden Seiten der Gleichungen (14), und findet so die Relation

(15) $$t^5 - 10 f t^3 + 45 f^2 t - T = 0,$$

oder auch

(16) $$t^2 (t^4 - 10 f t^2 + 45 f^2)^2 - T^2 = 0.$$

Aus (16) und (15) ergeben sich nun nach (10) und (12) die Gleichungen 5ten Grades für r und für u

(17) $$r (r^2 - 10 r + 45)^2 = z_1,$$

(18) $$u^5 - \frac{10 u^3}{z_1} + \frac{45 u}{z_1^2} - \frac{1}{z_1^2} = 0.$$

Die letzte dieser Gleichungen geht durch die Substitution

(19) $$y = -\frac{1}{3 u}, \quad z_1 = 27 \gamma$$

in die Form

(20) $$y^5 + 15 y^4 - 10 \gamma y^2 + 3 \gamma^2 = 0$$

über, die wir bereits im §. 75 des ersten Bandes als eine Normalform der Gleichung 5ten Grades kennen gelernt haben.

§. 112.

Die Hauptresolvente fünften Grades.

Wenn man die Functionen u, v gleichzeitig benutzt, so kann man eine Schaar von Resolventen ableiten, die die Form der Hauptgleichung 5ten Grades haben, und sich direct mit einer beliebig gegebenen Hauptgleichung 5ten Grades in Uebereinstimmung bringen lassen [1]).

Da es beim Ikosaëder keine Invarianten 8ten, 14ten, 16ten, 22sten oder 28sten Grades giebt, so müssen die Functionen $S(\bar\omega)$, $S(t\bar\omega)$, $S(\bar\omega^2)$, $S(t\bar\omega^2)$, $S(t^2\bar\omega^2)$ verschwinden, und wenn wir also

(1) $$Y = \alpha \bar\omega + \beta t \bar\omega$$

setzen, so werden auch die Functionen

$$S(Y), \quad S(Y^2)$$

für beliebige Werthe der Parameter α, β verschwinden, und daraus ergiebt sich eine identische Gleichung von der Form

1) Kiepert, Göttinger Nachrichten 1878. Crelle's Journal, Bd. 87. Klein, Ikosaëder, S. 106.

(2) $$Y^5 + 5a Y^2 + 5b Y + c = 0,$$

worin a, b, c homogene Functionen 3ten, 4ten, 5ten Grades von α, β bedeuten, deren Coëfficienten Ikosaëderinvarianten sind.

Die Function c können wir leicht aus der Formel bestimmen

$$c = -\Pi(\bar{\omega})\,\Pi(\alpha + \beta t).$$

Es ist nämlich nach (15) des vorigen Paragraphen für ein unbestimmtes λ

$$\lambda^5 - 10 f \lambda^3 + 45 f^2 \lambda - T = \Pi(\lambda - t),$$

also, wenn man $\lambda = -\alpha : \beta$ setzt

$$\Pi(\alpha + \beta t) \doteq \alpha^5 - 10 f \alpha^3 \beta^2 + 45 f^2 \alpha \beta^4 + T \beta^5,$$

und ferner ergiebt sich ohne Weiteres durch Vergleichung eines Gliedes [§. 111, (6), (8)]

$$\Pi(\bar{\omega}) = -H^2,$$

also

(3) $$c = H^2 (\alpha^5 - 10 f \alpha^3 \beta^2 + 45 f^2 \alpha \beta^4 + T \beta^5).$$

Die Coëfficienten a, b berechnet man wohl am einfachsten mit Hülfe der Newton'schen Formeln (Bd. I, §. 42):

$$-15 a = S(\alpha \bar{\omega} + \beta t \bar{\omega})^3$$
$$-20 b = S(\alpha \bar{\omega} + \beta t \bar{\omega})^4,$$

indem man die Formeln anwendet, die sich nach kurzer Rechnung durch Vergleichung je eines Gliedes der rechten und linken Seite ergeben:

$$S(\bar{\omega}^3) = -3.5.8 f^2, \qquad S(t\bar{\omega}^3) = -5T,$$
$$S(t^2\bar{\omega}^3) = -5.72 f^3, \qquad S(t^3\bar{\omega}^3) = -3.5 f T,$$
$$S(\bar{\omega}^4) = 4.5 f H, \qquad S(t^2\bar{\omega}^4) = -5.12 f^2 H,$$
$$S(t^3\bar{\omega}^4) = -5 H T, \qquad S(t^4\bar{\omega}^4) = -4.5.27 f^3 H.$$

So findet sich

(4) $$a = 8 f^2 \alpha^3 + T \alpha^2 \beta + 72 f^3 \alpha \beta^2 + f T \beta^3$$

(5) $$b = -f H \alpha^4 + 18 f^2 H \alpha^2 \beta^2 + H T \alpha \beta^3 + 27 f^3 H \beta^4.$$

Um daraus die Resolvente der Ikosaëdergleichung zu erhalten, müssen wir statt $\bar{\omega}$ und t die Functionen u, v [§. 111, (12)] einführen.

Setzen wir, indem wir mit λ, μ irgend zwei unbestimmte Grössen bezeichnen

(6) $$\alpha = \frac{\lambda f}{H}, \quad \beta = \frac{\mu f^3}{H T},$$

so folgt nach (1) und §. 111, (12):

(7) $$Y = \lambda v + \mu v u,$$

und wenn wir, wie in §. 111

(8) $$\frac{H^3}{f^5} = z, \quad \frac{T^2}{f^5} = z_1, \quad z + z_1 = 1728$$

setzen, so gehen die Ausdrücke (3), (4), (5) in folgende über:

(9) $$\begin{aligned} a z &= 8\lambda^3 + \lambda^2\mu + \frac{72\lambda\mu^2 + \mu^3}{z_1} \\ b z &= -\lambda^4 + \frac{18\lambda^2\mu^2 + \lambda\mu^3}{z_1} + 27\frac{\mu^4}{z_1^2} \\ c z &= \lambda^5 - 10\frac{\lambda^3\mu^2}{z_1} + \frac{45\lambda\mu^4 + \mu^5}{z_1^2}, \end{aligned}$$

wenn Y die Wurzel der Gleichung

(10) $$Y^5 + 5aY^2 + 5bY + c = 0$$

ist. Diese Gleichung hat die Form einer Hauptgleichung 5ten Grades, und sie kann jede Hauptgleichung darstellen, wenn wir a, b, c beliebig annehmen können. Man hat also, wenn a, b, c beliebig gegeben angenommen werden, aus (9) die drei Grössen λ, μ, z_1 (und $z = 1728 - z_1$) zu bestimmen, und es ist eine sehr merkwürdige Eigenthümlichkeit dieses Gleichungssystemes, dass sich diese Unbekannten rational durch die gegebenen Grössen a, b, c und die Discriminante der Gleichung (10) ausdrücken lassen.

Um dies nachzuweisen, leiten wir aus (9) zunächst einfachere Gleichungen ab.

Wenn wir die zweite von ihnen mit λ multipliciren und zur dritten addiren, so folgt

(11) $$z_1(\lambda b + c) = \mu^2 a,$$

und wenn wir die dritte mit λ, die zweite mit $\mu^2 : z_1$ multipliciren und subtrahiren

(12) $$z\left(\lambda c - \frac{\mu^2}{z_1} b\right) = \left(\lambda^2 - 3\frac{\mu^2}{z_1}\right)^3.$$

Ebenso ergiebt sich aus der ersten und zweiten

$$z\frac{a\lambda + 8b}{\mu} = \lambda^3 + \frac{216\lambda^2\mu}{z_1} + 9\frac{\lambda\mu^2}{z_1} + \frac{216\mu^3}{z_1^2}.$$

Diese Gleichung ergiebt, wenn man beiderseits zum Quadrat erhebt:

$$\begin{aligned} z_1 z^2 \left(\frac{a\lambda + 8b}{\mu}\right)^2 = \lambda^6 z_1 + 2.216\,\lambda^5\mu + \left(18 + \frac{216^2}{z_1}\right)\lambda^4\mu^2 \\ + \frac{2.2160}{z_1}\,\lambda^3\mu^3 + \left(\frac{81}{z_1} + \frac{2.216^2}{z_1^2}\right)\lambda^2\mu^4 \\ + \frac{18.216}{z_1^2}\,\lambda\,\mu^5 + \frac{216^2\mu^6}{z_1^3}, \end{aligned}$$

und wenn man dies abzieht von der aus der ersten Gleichung (9) abgeleiteten Formel:

$$\begin{aligned} 27\,a^2 z^2 = 1728\,\lambda^6 + 2.216\,\lambda^5\mu + 27\left(1 + \frac{16.72}{z_1}\right)\lambda^4\mu^2 \\ + \frac{2.2160}{z_1}\,\lambda^3\mu^3 + 27\left(\frac{2}{z_1} + \frac{72^2}{z_1^2}\right)\lambda^2\mu^4 \\ + \frac{18.216}{z_1^2}\,\lambda\,\mu^5 + \frac{27\,\mu^6}{z_1^2}, \end{aligned}$$

so folgt mit Rücksicht auf (8):

$$(13)\qquad z\left[27\,a^2 - z_1\left(\frac{a\lambda + 8b}{\mu}\right)^2\right] = \left(\lambda^2 - \frac{3\,\mu^2}{z_1}\right)^3.$$

Daraus ergiebt sich weiter durch Vergleichung mit (12)

$$(14)\qquad 27\,a^2 - \frac{z_1}{\mu^2}(a\lambda + 8b)^2 = \lambda c - \frac{\mu^2}{z_1}\,b,$$

und wenn man hieraus durch (11) das Verhältniss $\mu^2 : z_1$ eliminirt, so ergiebt sich die quadratische Gleichung für λ:

$$\begin{aligned} (15)\qquad \lambda^2(a^4 + abc - b^3) - \lambda\,(11\,a^3 b - a c^2 + 2\,b^2 c) \\ - 27\,a^3 c + 64\,a^2 b^2 - b c^2 = 0. \end{aligned}$$

Die Discriminante dieser quadratischen Gleichung ist

$$\begin{aligned} \Delta = (11\,a^3 b - a c^2 + 2\,b^2 c)^2 \\ + 4\,(a^4 + abc - b^3)(27\,a^3 c - 64\,a^2 b^2 + b c^2) \\ = a^2\,(108\,a^5 c - 135\,a^4 b^2 + 90\,a^2 b c^2 \\ - 320\,a b^3 c + 256\,b^5 + c^4). \end{aligned}$$

Im §. 74 des ersten Bandes ist die Discriminante D der Hauptgleichung 5ten Grades abgeleitet. Wenn man in der dort gefundenen Formel (3)

$$a_0 = 1,\quad a_3 = 5\,a,\quad a_4 = 5\,b,\quad a_5 = c$$

einsetzt, so findet sich

$$D = 5^5\,(108\,a^5 c - 135\,a^4 b^2 + 90\,a^2 b c^2 \\ - 320\,a b^3 c + 256\,b^5 + c^4),$$

so dass sich

(16) $$5^5 \varDelta = a^2 D$$

ergiebt, und man aus (15) für λ den Ausdruck

$$\lambda = \frac{11\,a^3 b - a c^2 + 2\,b^2 c + {}^1/_{25}\, a \sqrt{{}^1/_5\, D}}{2\,(a^4 + a b c - b^3)}$$

erhält, in dem die Quadratwurzel beide Vorzeichen haben kann.

Man sieht, dass ausser der Quadratwurzel aus der Discriminante, die rational durch die Wurzeln ausdrückbar ist, noch $\sqrt{5}$ darin vorkommt.

Hat man λ berechnet, so erhält man aus (11) das Verhältniss $z_1 : \mu^2$ und aus (12) die letzte Unbekannte z rational durch λ dargestellt.

§. 113.

Resolventen sechsten Grades.

Um die Resolventen 6ten Grades der Ikosaëdergleichung zu finden, gehen wir von einer der in der Ikosaëdergruppe enthaltenen Diëdergruppen D_5 aus (§. 111, 2.). Die Darstellung der Ikosaëdergruppe [§. 58, (20)] giebt uns unmittelbar die Zerlegung in die Nebengruppen; ist

(1) $$Q = \Theta^r,\quad \Theta^r \psi,\quad r = 0, 1, 2, 3, 4$$

die Diëdergruppe, von der wir ausgehen, so erhalten wir die volle Ikosaëdergruppe

(2) $$P = Q + Q\chi + Q\chi\Theta + Q\chi\Theta^2 + Q\chi\Theta^3 + Q\chi\Theta^4.$$

Ist dann U_∞ eine Function, die durch die Substitutionen von Q ungeändert bleibt und durch

$$\chi,\ \chi\Theta,\ \chi\Theta^2,\ \chi\Theta^3,\ \chi\Theta^4$$

in

$$U_0,\ U_1,\ U_2,\ U_3,\ U_4$$

übergeht, so sind die $U_\infty, U_0, U_1, U_2, U_3, U_4$ die Wurzeln einer Resolvente 6ten Grades. (Ueber die Bezeichnung U_∞ vgl. §. 65.)

Um die Galois'sche Gruppe dieser Gleichung 6ten Grades zu erhalten, haben wir den Einfluss zu untersuchen, den die Anwendung der Ikosaëdersubstitutionen auf das System der Nebengruppen (2) hat. Es genügt dazu, die Substitutionen Θ, ψ, χ zu betrachten. Es ist aber, wenn wir die Reihenfolge der Nebengruppen in (2) beachten, nach §. 58, (23), (25):

$$\begin{aligned} P\Theta &= Q + Q\chi\Theta + Q\chi\Theta^2 + Q\chi\Theta^3 + Q\chi\Theta^4 + Q\chi \\ P\psi &= Q + Q\chi + Q\chi\Theta^4 + Q\chi\Theta^3 + Q\chi\Theta^2 + Q\chi\Theta \\ P\chi &= Q\chi + Q + Q\chi\Theta + Q\chi\Theta^3 + Q\chi\Theta^2 + Q\chi\Theta^4, \end{aligned}$$

und daraus folgt, dass sich die Indices von U folgendermaassen vertauschen:

	∞,	0,	1,	2,	3,	4
Θ)	∞	1	2	3	4	0
ψ)	∞	0	4	3	2	1
χ)	0	∞	1	3	2	4.

Bezeichnen wir den Index allgemein mit ξ, und nehmen, wie im siebenten Abschnitte, ξ nach dem Modul 5, so dass zwei nach dem Modul 5 congruente Zahlen als nicht verschieden gelten, so können wir diese Vertauschungen so darstellen:

$$\Theta = (\xi, \xi + 1), \quad \psi = (\xi, -\xi), \quad \chi = \left(\xi, \frac{1}{\xi}\right).$$

Daraus folgt aber, dass die Gruppe unserer Gleichung 6ten Grades mit der Congruenzgruppe L_5 (§. 68) übereinstimmt.

Um zur Bildung von Resolventen 6ten Grades zu gelangen, müssen wir ähnlich wie bei den Resolventen 5ten Grades verfahren.

Wir haben schon im §. 55 die Grundformen der Diëdergruppen kennen gelernt. Wir stellen sie jetzt in der Form dar:

$$\varphi_1 = x_1 x_2, \quad \varphi_2 = x_1^5 + i x_2^5, \quad \varphi_3 = x_1^5 - i x_2^5.$$

Nehmen wir Θ und ψ mit der Determinante 1, also

$$\Theta = \begin{pmatrix} e^{\frac{\pi i}{5}}, & 0 \\ 0, & e^{-\frac{\pi i}{5}} \end{pmatrix}, \quad \psi = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix},$$

so ändern sich die Grundformen φ_1, φ_2, φ_3 in folgender Weise:

	φ_1	φ_2	φ_3
Θ)	φ_1	$-\varphi_2$	$-\varphi_3$
ψ)	$-\varphi_1$	$-i\varphi_2$	$i\varphi_3$.

Es sind also φ_1^2, φ_2^4, φ_3^4, $\varphi_2\,\varphi_3$ absolut invariant, und wenn wir daher, wie im §. 111, unter f, H, T die Ikosaëderinvarianten verstehen, so können wir folgende Functionen als Wurzeln von Resolventen 6ten Grades einführen:

$$\frac{\varphi_1^2 H}{f^2},\quad \frac{\varphi_2^4}{H},\quad \frac{\varphi_3^4}{H},\quad \frac{\varphi_2\,\varphi_3\,H}{T}.$$

Um die Ausdrücke für die übrigen Wurzeln zu erhalten, muss der Einfluss der mit der Determinante 1 genommenen Substitutionen $\Theta^r\chi$ auf die Functionen φ_1, φ_2, φ_3 untersucht werden. Wir wollen dies nur für die Function φ_1 durchführen, die zu der einfachsten Resolvente 6ten Grades führt.

Wenn wir in φ_1 die Substitution χ in der Form §. 58, (26) anwenden, also x_1, x_2 durch

$$\frac{x_1}{\varepsilon - \varepsilon^{-1}} + \frac{x_2}{\varepsilon^2 - \varepsilon^{-2}},\quad \frac{x_1}{\varepsilon^2 - \varepsilon^{-2}} - \frac{x_2}{\varepsilon - \varepsilon^{-1}}$$

ersetzen, so geht φ_1 in

$$\frac{-x_1^2 + x_1 x_2 + x_2^2}{\sqrt{5}}$$

über. Wir setzen demnach

(3) $$w_\infty = 5\,\varphi_1^2 = 5\,x_1^2 x_2^2,$$

und erhalten durch Anwendung der Substitutionen $\chi\,\Theta^r$ daraus die fünf weiteren Formen

(4) $$w_r = (\varepsilon^r x_1^2 + x_1 x_2 - \varepsilon^{-r} x_2^2)^2.$$

Nun sind die symmetrischen Functionen der sechs Formen w invariante Ikosaëderformen, und danach kann man leicht die Coëfficienten der Gleichung bilden, deren Wurzeln die w sind.

Wir erhalten durch Vergleichung der Grade und je eines Coëfficienten für die Potenzsummen der w

$$S(w) = 0,\quad S(w^2) = 0,\quad S(w^3) = 30 f,\quad S(w^4) = 0,\quad S(w^5) = -5\,H,$$

und so das Product aller sechs w

$$\Pi(w) = 5 f^2,$$

und demnach ergiebt sich nach den Newton'schen Formeln (Bd. I, §. 42) für w die Gleichung

(5) $$w^6 - 10 f w^3 + H w + 5 f^2 = 0.$$

Setzen wir also

(6) $$U = \frac{w H}{f^2},\quad z = \frac{H^3}{f^2},$$

so folgt hieraus die Gleichung 6ten Grades für U:

$$(7)\qquad U^6 - 10 z U^3 + z^2 U + 5 z^2 = 0$$

als Resolvente 6ten Grades der Ikosaëdergleichung.

Setzen wir nach (3) und (4)

$$(8)\qquad \begin{aligned} \sqrt{w_\infty} &= \sqrt{5}\, x_1 x_2 \\ \sqrt{w_r} &= \varepsilon^r x_1^2 + x_1 x_2 - \varepsilon^{-r} x_2^2, \end{aligned}$$

so ergeben sich daraus die folgenden Relationen:

$$(9)\qquad \begin{aligned} \sqrt{5 w_\infty} &= \sqrt{w_0} + \sqrt{w_1} + \sqrt{w_2} + \sqrt{w_3} + \sqrt{w_4} \\ 0 &= \sqrt{w_0} + \varepsilon^2 \sqrt{w_1} + \varepsilon^4 \sqrt{w_2} + \varepsilon \sqrt{w_3} + \varepsilon^3 \sqrt{w_4} \\ 0 &= \sqrt{w_0} + \varepsilon^3 \sqrt{w_1} + \varepsilon \sqrt{w_2} + \varepsilon^4 \sqrt{w_3} + \varepsilon^2 \sqrt{w_4} \end{aligned}$$

$$(10)\qquad \frac{x_1 \sqrt{5}}{x_2} = \frac{\sqrt{w_0} + \varepsilon^4 \sqrt{w_1} + \varepsilon^3 \sqrt{w_2} + \varepsilon^2 \sqrt{w_3} + \varepsilon \sqrt{w_4}}{\sqrt{w_\infty}},$$

und in den Gleichungen (9), (10) können, da sie homogen sind, an Stelle der w auch die U gesetzt werden.

Auf die Gleichungen 6ten Grades, deren Wurzeln den Relationen (9) genügen, hat zuerst Jacobi hingewiesen; man nennt sie daher Jacobi'sche Gleichungen 6ten Grades [1]).

§. 114.

Ueber die Lösung der Ikosaëdergleichung durch transcendente Functionen.

Wir wollen hier, ohne auf Beweise oder nähere Ausführungen einzugehen, kurz auf die Beziehungen hinweisen, die zwischen den durchgeführten Untersuchungen und der Theorie gewisser transcendenter Functionen, besonders der Theorie der elliptischen Functionen und der Theorie der hypergeometrischen Reihen bestehen, woraus sich die Auflösung der Ikosaëdergleichung und damit aller ihrer Resolventen durch transcendente Functionen ergiebt. Dies führt aus dem Gebiete der Algebra hinaus, steht aber zu ihr etwa in derselben Beziehung, wie wenn man bei der Berechnung von Wurzelgrössen Logarithmen, oder bei den cubischen Gleichungen die Winkeltheilung anwendet.

---

[1]) Suite des notices sur les fonctions elliptiques. Crelle's Journal, Bd. III (1828); Werke, Bd. I, S. 261.

Wir müssen uns hier auf eine kurze Angabe der Resultate beschränken, und werden in der Folge keine Anwendungen davon machen, so dass diese Ausführungen, die nur einem mit der Theorie der transcendenten Functionen einigermaassen vertrauten Leser ganz verständlich sein können, ohne Störung des Zusammenhanges auch übergangen werden können.

Es möge ω eine Variable bedeuten, deren imaginärer Theil positiv ist, so dass

(1) $$q = e^{\pi i \omega}$$

eine Grösse ist, deren absoluter Werth ein echter Bruch ist. Wir wollen die folgenden drei Functionen dieser Variablen ω betrachten:

(2) $$\eta(\omega) = q^{1/12} \prod_{1,\infty}^{\nu} (1 - q^{2\nu})$$
$$= q^{1/12} \sum_{-\infty,\infty}^{\nu} (-1)^{\nu} q^{3\nu^2+\nu} = \sum_{-\infty,\infty}^{\nu} (-1)^{\nu} q^{\frac{(6\nu+1)^2}{12}},$$

(3) $$f(\omega) = q^{-\frac{1}{24}} \prod (1 + q^{2\nu - 1}),$$

(4) $$\gamma_2(\omega) = \frac{f(\omega)^{24} - 16}{f(\omega)^8}\ ^{1)}.$$

In der Transformationstheorie der elliptischen Functionen[2]) wird eine Gleichung 6ten Grades abgeleitet, deren Wurzeln die sechs Grössen

(5) $$v_\infty = 5\left(\frac{\eta(5\omega)}{\eta(\omega)}\right)^2, \quad v_\xi = \left(\frac{\eta\left(\frac{-24\xi+\omega}{5}\right)}{\eta(\omega)}\right)^2$$

sind, wenn ξ ein volles Restsystem nach dem Modul 5 durchläuft. Diese Gleichung lautet

(6) $$v^6 + 10 v^3 - \gamma_2(\omega)\, v + 5 = 0,$$

und hat, wie man sieht, grosse Aehnlichkeit mit der im vorigen Paragraphen betrachteten Resolvente 6ten Grades

(7) $$U^6 - 10 z U^3 + z^2 U + 5 z^2 = 0.$$

Diese beiden Gleichungen gehen geradezu in einander über, wenn man

(8) $$z = \gamma_2(\omega)^3$$

(9) $$U = -\gamma_2(\omega)\, v$$

---

1) Man vergl.: Weber, „Elliptische Functionen und algebraische Zahlen". Braunschweig 1891. S. 63, 86, 149.

2) Ebend., S. 263, 316.

setzt. Die Gleichung (6) hat dieselbe Galois'sche Gruppe, wie (7). Wir können nun eine beliebige unter den Wurzeln von (7) für U_∞ setzen, und folglich können wir U_∞ und v_∞ in (9) einander entsprechen lassen. Dann können wir von den übrigen Wurzeln von (7) eine beliebige für U_0 nehmen, weil wir x_1, x_2 in §. 113, (4) durch $\varepsilon^r x_1$, $\varepsilon^{-r} x_2$ ersetzen können. Wir lassen also U_0 und v_0 einander entsprechen. Endlich können wir über die imaginäre fünfte Einheitswurzel ε noch so verfügen, dass U_1 und v_1 sich entsprechen, und dann folgt aus der Uebereinstimmung der Gruppe, dass überhaupt U_ξ und v_ξ sich entsprechen, dass also

$$(10)\qquad U_\xi = -\gamma_2(\omega)\, v_\xi, \quad \xi = \infty, 0, 1, 2, 3, 4$$

ist. Wenn wir also ω bei gegebenem z aus der transcendenten Gleichung (8) bestimmen, so geben uns (10) und (5) die vollständige Lösung der Ikosaëderresolvente 6ten Grades.

Nach (2) und (5) ergiebt sich für $\xi = 0, 1, 2, 3, 4$

$$(11)\qquad \eta(\omega)\sqrt{v_\xi} = \sum_{-\infty,\infty}^{\nu} (-1)^\nu e^{\frac{\pi i}{60}(\omega - 24\xi)(6\nu+1)^2}.$$

Der Exponent $(6\nu + 1)^2$ kann nach dem Modul 5 nur den Rest 0, 1, -1 geben. Lässt man also ν_1, ν_2 alle Zahlen durchlaufen, die den Bedingungen

$$\nu_1 \equiv 1, 2, \quad \nu_2 \equiv 0, 3 \pmod 5$$

genügen, so können wir den Ausdruck (11) so zerlegen:

$$(12)\qquad \eta(\omega)\sqrt{v_\xi} = \eta(5\omega) + \varepsilon^\xi \sum^{\nu_1} (-1)^{\nu_1} e^{\frac{\pi i}{60}\omega(6\nu_1+1)^2} + \varepsilon^{-\xi} \sum^{\nu_2} (-1)^{\nu_2} e^{\frac{\pi i}{60}\omega(6\nu_2+1)^2},$$

wenn $\varepsilon = e^{\frac{2\pi i}{5}}$ gesetzt ist. Hieraus erkennt man, dass die Grössen $\sqrt{v_\xi}$ die Relationen (9) des vorigen Paragraphen befriedigen, und die Formel (10), §. 113 ergiebt für die Wurzel $x = x_1 : x_2$ der Ikosaëdergleichung den Ausdruck:

$$(13)\qquad \eta(5\omega)\, x = \sum^{\nu_1} (-1)^{\nu_1} e^{\frac{\pi i}{60}\omega(6\nu_1+1)^2}.$$

Die übrigen Wurzeln erhält man, wenn man auf x die Ikosaëdersubstitutionen anwendet. Man kann sie aber auch da-

durch bilden, dass man die Variable ω durch einen äquivalenten Werth ersetzt (Bd. I, §. 120).

Wir wollen hier endlich auch noch die Lösung der Ikosaëdergleichung durch hypergeometrische Reihen kurz erwähnen. Nach Gauss verstehen wir unter

$$F(\alpha, \beta, \gamma, \xi)$$

die unendliche Reihe

$$1 + \frac{\alpha\beta}{1.\gamma}\xi + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1.2\,\gamma(\gamma+1)}\xi^2 + \frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{1.2.3\,\gamma(\gamma+1)(\gamma+2)}\xi^3 + \cdots$$

Setzen wir darin

$$z = 1728\,\xi,$$

so erhält die Wurzel der Ikosaëdergleichung

$$H^3 - z f^5 = 0$$

den Ausdruck

$$x = \xi^{\frac{1}{3}} \frac{F\left(\frac{11}{60}, \frac{19}{60}, \frac{4}{3}, \xi\right)}{F\left(\frac{11}{60}, \frac{-1}{60}, \frac{1}{3}, \xi\right)}.$$

Diese Reihen convergiren nur, so lange der absolute Werth von ξ ein echter Bruch ist, können aber für andere Werthe von ξ durch ähnliche Reihen ersetzt werden [1]).

---

[1]) H. A. Schwarz, „Ueber diejenigen Fälle, in denen die Gauss'sche Reihe $F(\alpha, \beta, \gamma, x)$ eine algebraische Function ihres vierten Elementes ist". Crelle's Journal, Bd. 75, 1872 (gesammelte mathematische Werke, Bd. II). F. Klein, Vorlesungen über das Ikosaëder, Abschnitt I, Cap. III.

Vierzehnter Abschnitt.

Gruppen linearer ternärer Substitutionen.

§. 115.

Ternäre lineare Substitutionsgruppe vom 168sten Grade.

Die Frage nach der Gesammtheit aller möglichen endlichen Gruppen linearer Substitutionen von mehreren, insbesondere derer von drei und vier Dimensionen, ist von C. Jordan behandelt, der, ähnlich wie es für die binären Substitutionen geschehen, eine endliche Anzahl von Typen solcher Gruppen aufgestellt hat [1]). Diese allgemeinen Untersuchungen können wir hier nicht verfolgen, wir begnügen uns, ein Beispiel einer ternären Gruppe ausführlicher zu betrachten.

In dem Abschnitte über die Congruenzgruppen (§. 66) haben wir eine Reihe einfacher Gruppen kennen gelernt, von denen sich die erste, vom Grade 60, als isomorph mit der Ikosaëdergruppe erwiesen hat. Wir wollen nun die nächste dieser einfachen Gruppen vom Grade 168 betrachten, die wir mit L_7 bezeichnet haben, und versuchen, eine mit dieser isomorphe, ternäre, lineare Substitutionsgruppe zu construiren.

Dazu führt uns das Theorem §. 72, I., wenn wir vier Elemente τ, χ, ω, Θ aufsuchen, die bei der Composition den Bedingungen dieses Theorems genügen.

Wir wollen zunächst eine Substitution τ in der Normalform annehmen

(1) $$\tau = \begin{pmatrix} \varepsilon_1, & 0, & 0 \\ 0, & \varepsilon_2, & 0 \\ 0, & 0, & \varepsilon_3 \end{pmatrix},$$

---

1) C. Jordan, Mémoire sur les équations différentielles linéaires à intégrale algébrique. Crelle's Journal für Mathematik, Bd. 84 (1878). Sur la détermination des groupes d'ordre fini etc. Atti della R. Accademia di Napoli, Vol. VIII (1879). Valentiner, Kjöb. Skrift (6) V (1889).

und darin müssen, da τ vom 7ten Grade sein soll, die $\varepsilon_1, \varepsilon_2, \varepsilon_3$ siebente Einheitswurzeln sein, die der Bedingung

$$(2) \qquad \varepsilon_1 \varepsilon_2 \varepsilon_3 = 1$$

genügen.

Nun wollen wir die Substitution χ so zu bestimmen suchen, dass die Bedingung $\chi \tau = \tau^4 \chi$ oder

$$(3) \qquad \tau \chi = \chi \tau^2$$

erfüllt ist. Nehmen wir χ in der Form

$$\chi = \begin{pmatrix} \alpha_1, \alpha_2, \alpha_3 \\ \beta_1, \beta_2, \beta_3 \\ \gamma_1, \gamma_2, \gamma_3 \end{pmatrix}$$

an, so ergiebt die Bedingung (3)

$$\begin{pmatrix} \alpha_1 \varepsilon_1, & \alpha_2 \varepsilon_1, & \alpha_3 \varepsilon_1 \\ \beta_1 \varepsilon_2, & \beta_2 \varepsilon_2, & \beta_3 \varepsilon_2 \\ \gamma_1 \varepsilon_3, & \gamma_2 \varepsilon_3, & \gamma_3 \varepsilon_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 \varepsilon_1^2, & \alpha_2 \varepsilon_2^2, & \alpha_3 \varepsilon_3^2 \\ \beta_1 \varepsilon_1^2, & \beta_2 \varepsilon_2^2, & \beta_3 \varepsilon_3^2 \\ \gamma_1 \varepsilon_1^2, & \gamma_2 \varepsilon_2^2, & \gamma_3 \varepsilon_3^2 \end{pmatrix}.$$

Da nun $\alpha_1, \beta_1, \gamma_1$ nicht alle drei verschwinden können, so muss ε_1^2 mit einer der drei Grössen $\varepsilon_1, \varepsilon_2, \varepsilon_3$ übereinstimmen. Wäre $\varepsilon_1 = \varepsilon_1^2$, also $\varepsilon_1 = 1$, und folglich $\varepsilon_3 = \varepsilon_2^{-1}$, so könnten weder ε_2 noch $\varepsilon_3 = 1$ sein, weil sonst τ die identische Substitution wäre. Es müsste also $\beta_1 = \gamma_1 = \alpha_2 = \alpha_3 = 0$ und $\varepsilon_2^2 = \varepsilon_3$, $\varepsilon_2^3 = 1$ sein, was unmöglich ist. Es bleiben daher nach (2) noch zwei mögliche Annahmen übrig:

$$\varepsilon_1 = \varepsilon, \quad \varepsilon_2 = \varepsilon^2, \quad \varepsilon_3 = \varepsilon^4,$$
$$\varepsilon_1 = \varepsilon, \quad \varepsilon_2 = \varepsilon^4, \quad \varepsilon_3 = \varepsilon^2,$$

worin ε eine imaginäre siebente Einheitswurzel ist, und diese beiden Annahmen führen zu zwei verschiedenen Gruppen, die ganz gleichartig gebaut, übrigens auch isomorph sind. Wir verfolgen hier die erste Annahme weiter, setzen also

$$(4) \quad \tau = \begin{pmatrix} \varepsilon, & 0, & 0 \\ 0, & \varepsilon^2, & 0 \\ 0, & 0, & \varepsilon^4 \end{pmatrix}, \quad \chi = \begin{pmatrix} 0, & 0, & 1 \\ 1, & 0, & 0 \\ 0, & 1, & 0 \end{pmatrix}, \quad \chi^2 = \begin{pmatrix} 0, & 1, & 0 \\ 0, & 0, & 1 \\ 1, & 0, & 0 \end{pmatrix}, \quad \chi^3 = 1.$$

Dass wir die nicht verschwindenden Grössen $\alpha_3, \beta_1, \gamma_2$ gleich 1 gesetzt haben, ist keine Beschränkung, da wir jede andere Annahme durch eine Transformation der ganzen Gruppe darauf zurückführen können.

Die Bedeutung von χ in dieser Form ist die einer cyklischen Permutation der Variablen. Die Substitutionen τ, χ erzeugen zusammen eine Gruppe $\tau^\varrho \chi^\lambda$ vom 21sten Grade.

Um nun ω zu bestimmen, bedienen wir uns der Relation

$$\omega\chi = \chi^2\omega,$$

und erhalten, wenn

$$\omega = \begin{pmatrix} \alpha_1, & \alpha_2, & \alpha_3 \\ \beta_1, & \beta_2, & \beta_3 \\ \gamma_1, & \gamma_2, & \gamma_3 \end{pmatrix}$$

gesetzt wird,

$$\begin{pmatrix} \alpha_2, & \alpha_3, & \alpha_1 \\ \beta_2, & \beta_3, & \beta_1 \\ \gamma_2, & \gamma_3, & \gamma_1 \end{pmatrix} = \begin{pmatrix} \beta_1, & \beta_2, & \beta_3 \\ \gamma_1, & \gamma_2, & \gamma_3 \\ \alpha_1, & \alpha_2, & \alpha_3 \end{pmatrix},$$

also

$$\alpha_1 = \beta_3 = \gamma_2 = \alpha,$$
$$\alpha_2 = \beta_1 = \gamma_3 = \beta,$$
$$\alpha_3 = \beta_2 = \gamma_1 = \gamma,$$

und ω erhält also die Form

(5) $$\omega = \begin{pmatrix} \alpha, & \beta, & \gamma \\ \beta, & \gamma, & \alpha \\ \gamma, & \alpha, & \beta \end{pmatrix}.$$

Drücken wir die Bedingung aus, dass ω vom 2ten Grade sein soll, so ergeben sich die Relationen

(6) $$\alpha^2 + \beta^2 + \gamma^2 = 1$$
$$\beta\gamma + \gamma\alpha + \alpha\beta = 0.$$

Aus (6) ergiebt sich $(\alpha + \beta + \gamma)^2 = 1$, und wenn man die Determinante von ω gleich 1 setzt, so folgt mit Benutzung von (6) $(\alpha + \beta + \gamma)^3 = -1$, folglich

(7) $$\alpha + \beta + \gamma = -1.$$

Aus (6) und (7) folgern wir noch die Relationen:

(8) $$\alpha = \beta\gamma - \alpha^2, \quad \beta = \gamma\alpha - \beta^2, \quad \gamma = \alpha\beta - \gamma^2$$

(9) $$\alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma = -1,$$

von denen die letztere, die man aus

$$(\alpha + \beta + \gamma)^3 - 3(\beta\gamma + \gamma\alpha + \alpha\beta)(\alpha + \beta + \gamma) = -1$$

erhält, den negativen Werth der Determinante von ω darstellt.

Endlich bilden wir noch nach den Relationen [§. 72, (15)]

$$\Theta = \chi\tau^3\omega\tau^4, \quad \Theta^3 = \chi\tau^6\omega\tau^2:$$

(10) $$\Theta = \begin{pmatrix} \gamma\varepsilon^2, & \alpha\varepsilon^6, & \beta \\ \alpha, & \beta\varepsilon^4, & \gamma\varepsilon^5 \\ \beta\varepsilon^3, & \gamma, & \alpha\varepsilon \end{pmatrix}, \quad \Theta^{-1} = \begin{pmatrix} \gamma\varepsilon^5, & \alpha, & \beta\varepsilon^4 \\ \alpha\varepsilon, & \beta\varepsilon^3, & \gamma \\ \beta, & \gamma\varepsilon^2, & \alpha\varepsilon^6 \end{pmatrix}.$$

Wenn wir nun die Bedingung aufsuchen, dass $\Theta^4 = 1$ wird, so haben wir $\Theta^2 = \Theta^{-2}$ zu setzen. Bilden wir also Θ^2 und Θ^{-2} nach (10), so kann man zuerst versuchen, die Uebereinstimmung herzustellen, indem man eine der drei Zahlen α, β, γ, etwa $\gamma = 0$, setzt; dann muss aber nach (6) und (7) noch eine zweite, etwa $\beta = 0$, und die dritte $\alpha = -1$ sein. Dann wird aber Θ^2 nicht mit Θ^{-2} übereinstimmend. Also sind alle drei Grössen α, β, γ von Null verschieden. Setzen wir nun das zweite und dritte Glied der ersten Zeile in den aus (10) abgeleiteten Substitutionen Θ^2 und Θ^{-2} einander gleich, so ergiebt sich, wenn die Factoren γ und α abgeworfen werden:

$$\alpha(\varepsilon - \varepsilon^{-2}) = \beta(\varepsilon^{-1} - 1), \quad \gamma(\varepsilon^4 - 1) = \beta(\varepsilon^3 - \varepsilon)$$

oder

$$\alpha(\varepsilon^2 - \varepsilon^{-2}) = \beta(\varepsilon^4 - \varepsilon^{-4}), \quad \gamma(\varepsilon^2 - \varepsilon^{-2}) = \beta(\varepsilon - \varepsilon^{-1}),$$

und hieraus, wenn h einen unbestimmten Factor bedeutet:

(11)
$$\begin{aligned} \alpha &= h\,(\varepsilon^4 - \varepsilon^{-4}) \\ \beta &= h\,(\varepsilon^2 - \varepsilon^{-2}) \\ \gamma &= h\,(\varepsilon - \varepsilon^{-1}). \end{aligned}$$

Der Factor h wird nach (7) aus der Gleichung

(12)
$$-1 = h\,(\varepsilon + \varepsilon^2 + \varepsilon^4 - \varepsilon^{-1} - \varepsilon^{-2} - \varepsilon^{-4})$$

bestimmt, und es ergiebt sich nach Bd. I, §. 171

(13)
$$h = \frac{i}{\sqrt{7}} = \frac{-1}{\sqrt{-7}}.$$

Das Vorzeichen von $\sqrt{7}$ hängt von der Wahl von ε ab und ist positiv, wenn z. B.

$$\varepsilon = e^{\frac{2\pi i}{7}}$$

genommen wird. Dann erhält man für α, β, γ

$$\alpha = \frac{-2\sin\frac{8\pi}{7}}{\sqrt{7}}, \quad \beta = \frac{-2\sin\frac{4\pi}{7}}{\sqrt{7}}, \quad \gamma = \frac{-2\sin\frac{2\pi}{7}}{\sqrt{7}}.$$

Aus (11) und (12) ergeben sich noch die Formeln

(14)
$$\begin{aligned} \alpha\,\varepsilon + \beta\,\varepsilon^4 + \gamma\,\varepsilon^2 &= 1 \\ \alpha\,\varepsilon^{-1} + \beta\,\varepsilon^{-4} + \gamma\,\varepsilon^{-2} &= 1, \\ \alpha + \beta\,\varepsilon^{-1} + \gamma\,\varepsilon^2 &= 0 \\ \alpha + \beta\,\varepsilon + \gamma\,\varepsilon^{-2} &= 0, \\ \alpha\beta\gamma &= \tfrac{1}{7}, \end{aligned}$$

und α, β, γ sind die Wurzeln der cubischen Gleichung

$$\alpha^3 + \alpha^2 - \tfrac{1}{7} = 0.$$

Man kann nun nach §. 72, (15), (12), (13)

$$(15) \qquad \Theta^2 = \tau^4 \omega \tau^5 \chi$$

setzen, und daraus erhält man leicht nach (4) und (5)

$$(16) \qquad \Theta^2 = \begin{pmatrix} \beta, & \gamma\varepsilon^3, & \alpha\varepsilon^2 \\ \gamma\varepsilon^{-3}, & \alpha, & \beta\varepsilon^{-1} \\ \alpha\varepsilon^{-2}, & \beta\varepsilon, & \gamma \end{pmatrix}.$$

Vergleicht man dies mit dem Resultate, was man erhält, wenn man aus (10) direct Θ^2 bildet, so ergiebt sich:

$$(17) \quad \begin{array}{ll} \alpha = \alpha^2\varepsilon^{-1} + \beta^2\varepsilon + \gamma^2\varepsilon^{-2}, & \alpha = \beta\gamma + \gamma\alpha\varepsilon^2 + \alpha\beta\varepsilon^{-1} \\ \beta = \alpha^2\varepsilon^{-1} + \beta^2\varepsilon^3 + \gamma^2\varepsilon^{-3}, & \beta = \beta\gamma\varepsilon^3 + \gamma\alpha + \alpha\beta\varepsilon \\ \gamma = \alpha^2\varepsilon^2 + \beta^2\varepsilon^3 + \gamma^2\varepsilon^{-2}, & \gamma = \beta\gamma\varepsilon^{-3} + \gamma\alpha\varepsilon^{-2} + \alpha\beta, \end{array}$$

und die Vergleichung mit dem aus (10) gebildeten Θ^{-2} ergiebt ein ganz ähnliches Formelsystem, das aus (17) hervorgeht, wenn ε mit ε^{-1} vertauscht wird, nämlich:

$$\begin{array}{ll} \alpha = \alpha^2\varepsilon + \beta^2\varepsilon^{-1} + \gamma^2\varepsilon^2, & \alpha = \beta\gamma + \gamma\alpha\varepsilon^{-2} + \alpha\beta\varepsilon \\ \beta = \alpha^2\varepsilon + \beta^2\varepsilon^{-3} + \gamma^2\varepsilon^3, & \beta = \beta\gamma\varepsilon^{-3} + \gamma\alpha + \alpha\beta\varepsilon^{-1} \\ \gamma = \alpha^2\varepsilon^{-2} + \beta^2\varepsilon^{-3} + \gamma^2\varepsilon^2, & \gamma = \beta\gamma\varepsilon^3 + \gamma\alpha\varepsilon^2 + \alpha\beta. \end{array}$$

Damit aber hierin kein Cirkelschluss liege, ist zu zeigen, dass die Relationen (17) in Folge der Bestimmungen (11), (12) wirklich erfüllt sind, denn dann erst ist das Bestehen der Relation (15) und die Gleichheit von Θ^2 mit Θ^{-2} nachgewiesen. Es genügt dazu, zwei dieser Relationen, etwa

$$\begin{array}{l} \alpha = \alpha^2\varepsilon^{-1} + \beta^2\varepsilon + \gamma^2\varepsilon^{-2} \\ \alpha = \beta\gamma + \gamma\alpha\varepsilon^2 + \alpha\beta\varepsilon^{-1}, \end{array}$$

abzuleiten; denn hat man diese nachgewiesen, so kann man darin ε mit ε^{-1} vertauschen, wodurch α, β, γ nicht geändert werden, und sodann ε mit ε^2 und ε^4, wodurch α, β, γ in γ, α, β und in β, γ, α übergehen; und daher erhält man das ganze Formelsystem (17).

Diese beiden Relationen ergeben sich aber durch eine einfache Rechnung nach (11), (12) in der Form:

$$\begin{array}{l} -(\varepsilon + \varepsilon^2 + \varepsilon^4 - \varepsilon^{-1} - \varepsilon^{-2} - \varepsilon^{-4})(\varepsilon^4 - \varepsilon^{-4}) \\ = \varepsilon^{-1}(\varepsilon^4 - \varepsilon^{-4})^2 + \varepsilon(\varepsilon^2 - \varepsilon^{-2})^2 + \varepsilon^{-2}(\varepsilon - \varepsilon^{-1})^2 \\ = (\varepsilon - \varepsilon^{-1})(\varepsilon^2 - \varepsilon^{-2}) + \varepsilon^2(\varepsilon - \varepsilon^{-1})(\varepsilon^4 - \varepsilon^{-4}) \\ \qquad + \varepsilon^{-1}(\varepsilon^2 - \varepsilon^{-2})(\varepsilon^4 - \varepsilon^{-4}). \end{array}$$

Aus diesen Formeln ergiebt sich leicht nach (5), (8), (14):

(18)
$$\omega\Theta = \begin{pmatrix} \gamma, & \alpha\varepsilon^{-2}, & \beta\varepsilon \\ \alpha\varepsilon^{2}, & \beta, & \gamma\varepsilon^{3} \\ \beta\varepsilon^{-1}, & \gamma\varepsilon^{-3}, & \alpha \end{pmatrix}, \quad \omega\Theta^2 = \begin{pmatrix} \gamma, & \alpha\varepsilon, & \beta\varepsilon^{3} \\ \alpha\varepsilon^{-1}, & \beta, & \gamma\varepsilon^{2} \\ \beta\varepsilon^{-3}, & \gamma\varepsilon^{-2}, & \alpha \end{pmatrix},$$
$$\Theta\omega = \omega\Theta^3 = \begin{pmatrix} \alpha, & \beta\varepsilon^{-1}, & \gamma\varepsilon^{-3} \\ \beta\varepsilon, & \gamma, & \alpha\varepsilon^{-2} \\ \gamma\varepsilon^{3}, & \alpha\varepsilon^{2}, & \beta \end{pmatrix}.$$

Hiernach ist es nun sehr einfach, die charakteristischen Relationen des Theorems I., §. 72 für unsere Gruppe durch wirkliche Ausrechnung zu bestätigen, und damit ist also die ternäre Gruppe 168sten Grades hergestellt [1]).

§. 116.

Pole und Axen der ternären Gruppen.

Wir wollen uns jetzt der Kürze halber einer geometrischen Ausdrucksweise bedienen, indem wir die Variablen x_1, x_2, x_3 als Dreieckscoordinaten eines Punktes x in einer Ebene betrachten, obwohl auch imaginäre Werthe von x_1, x_2, x_3 zulässig sein sollen.

Bedeutet A eine ternäre lineare Substitution mit der Determinante 1, und ist

(1) $$(y) = A(x),$$

so sind y_1, y_2, y_3 die Coordinaten eines zweiten Punktes (y), bezogen auf dasselbe Coordinatensystem, der aus (x) durch die Substitution A abgeleitet ist.

Wenn x eine gerade Linie durchläuft, so durchläuft auch y eine gerade Linie, und wenn die Gleichungen dieser beiden Linien

(2) $$u_1 x_1 + u_2 x_2 + u_3 x_3 = 0, \quad v_1 y_1 + v_2 y_2 + v_3 y_3 = 0$$

sind, so ergiebt sich durch Einsetzen von (1) in (2), dass u_1, u_2, u_3 mit v_1, v_2, v_3 durch die transponirte Substitution von A:

$$(u) = A_1(v)$$

[1]) Vergl. F. Klein, „Ueber die Transformation siebenter Ordnung der elliptischen Functionen". „Ueber die Auflösung gewisser Gleichungen vom 7ten und 8ten Grade". Mathem. Annalen, Bd. 14 u. 15. Klein-Fricke, Vorlesungen über Modul-Functionen, Bd. I, dritter Abschnitt, Capitel VII. Gordan, „Ueber Gleichungen 7ten Grades mit einer Gruppe von 168 Substitutionen". Mathem. Annalen, Bd. 20, 25.

zusammenhängen (§. 37, 9.). Es wird also durch A nicht nur aus jedem Punkte ein Punkt, sondern auch aus jeder geraden Linie eine gerade Linie abgeleitet.

Die durch (1) ausgedrückte Beziehung der Punkte y zu den Punkten x kann als eine Abbildung der Ebene in sich selbst bezeichnet werden, wobei jedem Punkte ein bestimmter anderer Punkt und jeder geraden Linie eine gerade Linie entspricht. Eine solche Abbildung heisst in der Geometrie auch eine Collineation. Der Punkt y heisst das Bild des Punktes x und die gerade Linie v das Bild der geraden Linie u. Hat man die Bilder zweier Punkte, so ist die Verbindungslinie dieser Bilder das Bild der Verbindungslinie der beiden Originalpunkte.

Bedeutet S eine zweite ternäre lineare Substitution und

$$A' = S^{-1} A S$$

die aus A durch S transformirte Substitution, so ist

$$(y') = A'(x')$$

gleichbedeutend mit

$$(y) = A(x),$$

wenn

$$(y) = S(y'), \quad (x) = S(x')$$

gesetzt wird. Statt nun durch S eine Abbildung zu definiren, kann man auch eine Coordinatentransformation darunter verstehen, indem man unter x_1', x_2', x_3' die Coordinaten des Punktes (x) in einem neuen, durch S bestimmten Coordinatensysteme versteht. Dann wird der Zusammenhang zwischen den beiden Punkten x, y ebenso wie durch A auch durch die transformirte Substitution A' ausgedrückt, und die Transformation der Substitutionen ist also gleichbedeutend mit der Transformation des Coordinatensystems. Die Composition der transformirten Substitutionen geschieht, wie wir schon früher gesehen haben, ebenso wie die der ursprünglichen, und es entsteht also durch Transformation aus jeder Gruppe eine isomorphe Gruppe.

Von grosser Wichtigkeit ist nun die Untersuchung der Punkte, die bei der Abbildung durch eine Substitution A ungeändert bleiben.

Nehmen wir A in der Form an:

$$A = \begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{pmatrix},$$

so erhalten wir als Bedingung dafür, dass der Punkt y mit dem Punkte x zusammenfällt, da ein Punkt durch die Verhältnisse seiner Coordinaten eindeutig bestimmt ist, die, dass für einen passend bestimmten Coëfficienten λ:

$$(3)\qquad \begin{aligned} \lambda x_1 &= \alpha\, x_1 + \beta\, x_2 + \gamma\, x_3 \\ \lambda x_2 &= \alpha' x_1 + \beta' x_2 + \gamma' x_3 \\ \lambda x_3 &= \alpha'' x_1 + \beta'' x_2 + \gamma'' x_3, \end{aligned}$$

woraus man durch Elimination von x_1, x_2, x_3 die cubische Gleichung für λ erhält:

$$(4)\qquad \varDelta = \begin{vmatrix} \alpha - \lambda, & \beta, & \gamma \\ \alpha', & \beta' - \lambda, & \gamma' \\ \alpha'', & \beta'', & \gamma'' - \lambda \end{vmatrix} = 0.$$

Es giebt daher im Allgemeinen drei Punkte, die ihre eigenen Bilder sind, und diese wollen wir (wie bei den binären Substitutionen) die Pole der Substitution A nennen. Die drei Verbindungslinien dieser Pole sind dann gleichfalls ihre eigenen Bilder, jedoch so, dass auf jeder dieser drei Geraden nur zwei Punkte liegen, die auf sich selbst abgebildet sind. Die Bilder der übrigen Punkte sind in der Linie verschoben. Diese Linien wollen wir die Axen der Substitution A nennen.

Es können nun aber besondere Fälle eintreten, die hervorzuheben sind. Es können zwei oder selbst alle drei Pole in einen Punkt zusammenfallen, wie das Beispiel

$$\begin{pmatrix} \alpha & 0 & 0 \\ \alpha' & \alpha & 0 \\ \alpha'' & \beta'' & \alpha^{-2} \end{pmatrix}$$

zeigt. Hier fallen, wenn $\alpha', \alpha'', \beta''$ von Null verschieden sind, zwei, oder wenn $\alpha = 1$ ist, alle drei Pole in einen Punkt zusammen.

Wichtiger noch ist ein anderer besonderer Fall, nämlich der, dass unendlich viele Punkte ihre eigenen Bilder sind. Wenn wir von dem Falle absehen, dass alle Punkte ihre eigenen Bilder sind, der nur bei der Multiplication vorkommt, so müssen die Punkte, die ihre eigenen Bilder sind, wenn ihrer unendlich viele sind, auf einer geraden Linie liegen; denn es kann dieser Fall nur dann eintreten, wenn für eine Wurzel von (4) die drei Gleichungen (3) aus einer von ihnen folgen, oder, was dasselbe ist, wenn mit $\varDelta$ zugleich die sämmtlichen ersten Unterdeterminanten

verschwinden. Eine solche gerade Linie wollen wir eine **Hauptaxe der Substitution** A nennen. Aber nur gewisse besondere Substitutionen besitzen Hauptaxen. Eine Substitution mit einer Hauptaxe hat ausser dieser noch **einen** Pol, der in besonderen Fällen auch in die Hauptaxe hineinfallen kann.

Legen wir, um diese Verhältnisse zu übersehen, die Hauptaxe in die Linie $x_1 = 0$, so muss, wenn $x_1 = 0$ ist, $y_1 = 0$, $y_2 : y_3 = x_2 : x_3$ sein. Daraus ergiebt sich

$$\begin{aligned} y_1 &= \alpha\, x_1 \\ y_2 &= \alpha' x_1 + \beta\, x_2 \\ y_3 &= \alpha'' x_1 + \beta\, x_3. \end{aligned}$$

Den ausser der Hauptaxe existirenden Pol erhalten wir, wenn wir $y_1 = \alpha x_1$, $y_2 = \alpha x_2$, $y_3 = \alpha x_3$ setzen; dann ergiebt sich

$$(\beta - \alpha)\, x_2 + \alpha' x_1 = 0, \quad (\beta - \alpha)\, x_3 + \alpha'' x_1 = 0,$$

und dieser Punkt wird dann und nur dann in die Linie $x_1 = 0$ fallen, wenn $\beta = \alpha$ ist. Dieser Fall kann bei endlichen Gruppen nicht eintreten (ausser bei der Multiplication).

Wenn ein von der Hauptaxe verschiedener Pol existirt, so können wir diesen in die Ecke $x_2 = 0$, $x_3 = 0$ legen, und die Substitution erhält die Form

$$y_1 = \alpha x_1, \quad y_2 = \beta x_2, \quad y_3 = \beta x_3,$$

wo α von β verschieden ist.

Eine gerade Linie $u_1 x_1 + u_2 x_2 + u_3 x_3 = 0$ ist dann und nur dann ihr eigenes Bild, wenn entweder $u_2 = u_3 = 0$ oder $u_1 = 0$ ist.

Wenn also eine Substitution einen Pol und eine Hauptaxe hat, so bleiben ausser dieser alle geraden Linien und nur die ungeändert, die durch den Pol gehen.

Es ist noch zu bemerken, dass, wenn drei getrennte Pole vorhanden sind, diese nicht in eine gerade Linie fallen können, ohne dass die Linie zur Hauptaxe wird. Denn wenn eine gerade Linie ihr eigenes Bild ist, so können, wenn sich die Linie nicht Punkt für Punkt selbst entspricht, nur zwei Punkte auf ihr liegen, die ihr eigenes Bild sind.

Fassen wir dies Alles zusammen, so finden wir folgende Arten von ternären linearen Substitutionen, wobei zusammenfallende Pole nur einmal mitgezählt sind:

1. Substitutionen mit drei Polen,
2. „ „ zwei Polen,
3. „ „ einem Pol,
4. „ „ einer Hauptaxe und einem Pol,
5. „ „ einer Hauptaxe.

Als letzter Fall würde noch die Multiplication aufzuzählen sein, für den jeder beliebige Punkt sein eigenes Bild ist.

Die Art der Substitution bleibt erhalten bei jeder Transformation.

Wenn ein Punkt ungeändert bleibt durch eine Substitution A, so bleibt er auch bei jeder Wiederholung von A, also bei $A^2, A^3, \ldots$, ungeändert. Die Pole von A finden sich daher immer unter den Punkten, die bei der Abbildung durch A^2 ihre eigenen Bilder sind. Es kann aber wohl der Fall eintreten, dass z. B. A drei Pole hat, während eine Potenz, A^k, eine Hauptaxe besitzt. Dann müssen zwei der Pole von A auf der Hauptaxe von A^k liegen, und der dritte Pol von A ist der einzelne Pol von A^k. Ist nämlich A eine Substitution mit drei Polen, so können wir sie, indem wir die Pole in die Ecken des Coordinatendreiecks legen, in die Normalform

$$A = \begin{pmatrix} \alpha, & 0, & 0 \\ 0, & \beta, & 0 \\ 0, & 0, & \gamma \end{pmatrix}$$

setzen, worin α, β, γ von einander verschieden sind. Ist nun $\beta^k = \gamma^k$, also β von γ um eine k^{te} Einheitswurzel als Factor unterschieden, so hat A^k die Linie $x_1 = 0$ zur Axe, und die gegenüberliegende Ecke des Coordinatendreiecks zum Pol.

Ist A von endlichem Grade μ, so sind α, β, γ μ^{te} Einheitswurzeln. Ist A^k die niedrigste Potenz von A, die eine Hauptaxe hat, so muss $\beta : \gamma$ primitive k^{te} und zugleich μ^{te} Einheitswurzel sein, und folglich muss k ein echter Theiler von μ sein; wenn k relativ prim zu μ ist, so hat A^k dieselben drei Pole wie A.

§. 117.

Anwendung auf die Gruppe G_{168}. Siebenzählige Pole.

Wir wollen nun die Pole und Axen der Substitutionen unserer Gruppe G_{168} aufsuchen.

Diese Arbeit wird wesentlich dadurch erleichtert, dass uns aus der Betrachtung der Congruenzgruppe L_7 die Grade und Cykeln der Gruppe schon bekannt sind (§. 68). Danach giebt es $p^2 - 1 = 48$ Elemente 7ten Grades A_7, $\frac{1}{4} p (p-3)(p+1) = 56$ Elemente 3ten Grades A_3 und $\frac{1}{4} p (p-1)^2 = 63$ Elemente 4ten oder 2ten Grades A_4, A_2 in G_{168}.

Die Elemente A_7 ordnen sich (mit Zuziehung der identischen Substitution) in acht Cykeln von sieben Gliedern, die A_3 in 28 Cykeln von drei Elementen und die A_4 und A_2 in 21 Cykeln von vier Gliedern. Jeder dieser letzteren Cykeln enthält ein Element A_2 und zwei Elemente A_4, und wenn wir also zusammenfassen, so erhalten wir:

48	Elemente	7ten	Grades
56	„	3ten	„
42	„	4ten	„
21	„	2ten	„ .

Wenn ein Punkt durch ν Substitutionen der Gruppe (die identische eingeschlossen) ungeändert bleibt, so wollen wir einen solchen Punkt einen ν-zähligen Pol nennen (§. 52).

Für die Feststellung der Pole und Axen genügt die Betrachtung je eines Cyklus, da aus diesem die anderen durch Transformation abgeleitet sind (§. 69).

Nehmen wir die Substitution 7ten Grades τ [§. 115, (4)], so finden wir die Ecken des Coordinatendreiecks als drei getrennte Pole. Alle Potenzen von τ, deren Exponenten nicht durch 7 theilbar sind, haben dieselben drei Pole.

Durch Anwendung der Substitutionen χ, χ^2 auf die Coordinaten dieser drei Pole gehen dieselben cyklisch in einander über; wendet man aber die Substitutionen Θ, Θ^2, Θ^3, ω, $\omega\Theta$, $\omega\Theta^2$, $\omega\Theta^3$ an, die in §. 115, (5), (10), (16), (18) vollständig gebildet sind, so geht das ganze Coordinatendreieck in ein völlig davon verschiedenes über (z. B. durch ω in das Dreieck mit den Eckcoordinaten α, β, γ; β, γ, α; γ, α, β), und daraus ist zu schliessen, dass diese Pole nicht mehr als siebenzählig sind. Es giebt acht Tripel solcher siebenzähliger Pole, die alle von einander verschieden sind, und jeder von ihnen kann in jeden anderen durch eine Substitution der Gruppe G_{168} transformirt werden.

Wir haben also den Satz:

1. **Es giebt 24 siebenzählige Pole, die sich, den acht siebengliedrigen Cykeln entsprechend, in acht Tripel theilen. Jeder dieser 24 Punkte kann in jeden anderen durch Substitutionen der Gruppe G_{168} transformirt werden.**

§. 118.

Die Hauptaxen.

Wir gehen zur Betrachtung der Substitutionen 4ten und 2ten Grades über, als deren Repräsentanten wir Θ und Θ^2 wählen. Nach §. 115, (10) und §. 116 haben wir für Θ die cubische Gleichung zu lösen:

$$(1) \qquad \begin{vmatrix} \gamma\varepsilon^2 - \lambda, & \alpha\varepsilon^6, & \beta \\ \alpha, & \beta\varepsilon^4 - \lambda, & \gamma\varepsilon^5 \\ \beta\varepsilon^3, & \gamma, & \alpha\varepsilon - \lambda \end{vmatrix} = 0,$$

die entwickelt so lautet:

$$(2) \qquad \begin{aligned} &\lambda^3 - \lambda^2(\alpha\varepsilon + \beta\varepsilon^4 + \gamma\varepsilon^2) \\ &- \lambda\,[\varepsilon^6(\alpha^2 - \beta\gamma) + \varepsilon^3(\beta^2 - \gamma\alpha) + \varepsilon^5(\gamma^2 - \alpha\beta)] \\ &+ \alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma = 0. \end{aligned}$$

Diese Gleichung reducirt sich aber mit Benutzung der Relationen (8), (9), (14) des §. 115 auf

$$(3) \qquad \lambda^3 - \lambda^2 + \lambda - 1 = 0,$$

und hat die Wurzeln

$$\lambda = 1, \quad \lambda = \pm i,$$

und daraus lassen sich die Coordinaten der drei Pole berechnen, die sich als rationale Functionen von ε und i ergeben.

Für die Pole von Θ^2 erhalten wir nach §. 115, (16) zunächst die cubische Gleichung

$$\begin{vmatrix} \beta - \lambda, & \gamma\varepsilon^3, & \alpha\varepsilon^2 \\ \gamma\varepsilon^{-3}, & \alpha - \lambda, & \beta\varepsilon^{-1} \\ \alpha\varepsilon^{-2}, & \beta\varepsilon, & \gamma - \lambda \end{vmatrix} = 0,$$

die nach den Relationen zwischen α, β, γ leicht in die Form

$$(4) \qquad (\lambda + 1)^2(\lambda - 1) = 0$$

gebracht wird und daher eine Doppelwurzel $\lambda = -1$ und eine einfache Wurzel $\lambda = 1$ hat. Setzen wir den Werth $\lambda = -1$

in die Gleichungen ein, durch die der ungeänderte Punkt bestimmt wird [§. 116, (3)], so ergiebt sich:

$$\begin{aligned}(\beta + 1)\, x_1 + \gamma\, \varepsilon^3\, x_2 + \alpha\, \varepsilon^2\, x_3 &= 0,\\ \gamma\, \varepsilon^{-3}\, x_1 + (\alpha + 1)\, x_2 + \beta\, \varepsilon^{-1}\, x_3 &= 0,\\ \alpha\, \varepsilon^{-2}\, x_1 + \beta\, \varepsilon\, x_2 + (\gamma + 1)\, x_3 &= 0.\end{aligned}$$

Diese drei Gleichungen reduciren sich alle auf die eine, die man z. B. aus der ersten durch Multiplication mit β und Anwendung von §. 115, (8) ableitet:

$$\alpha\gamma\, x_1 + \beta\gamma\, \varepsilon^3 x_2 + \alpha\beta\, \varepsilon^2 x_3 = 0, \tag{5}$$

und die eine gerade Linie darstellt. Diese Linie ist also eine Hauptaxe.

Solcher Hauptaxen erhalten wir 21, da wir 21 Substitutionen 2ten Grades haben.

Man kann die Functionen, die, gleich Null gesetzt, die 21 Hauptaxen darstellen, aus (5) leicht bilden, wenn man die Function

$$A = \alpha\gamma\, x_1 + \beta\gamma\, \varepsilon^3 x_2 + \alpha\beta\, \varepsilon^2 x_3 \tag{6}$$

durch die Substitutionen τ^r, $\tau^r\chi$, $\tau^r\chi^2$ transformirt ($r = 0, 1, 2, 3, 4, 5, 6$). Man erhält so die 21 Functionen:

$$\begin{aligned}A_{1,r} &= \alpha\gamma\, \varepsilon^r x_1 + \gamma\beta\, \varepsilon^{2r+3} x_2 + \alpha\beta\, \varepsilon^{4r+2} x_3\\ A_{2,r} &= \beta\gamma\, \varepsilon^{r+3} x_1 + \alpha\beta\, \varepsilon^{2r+2} x_2 + \alpha\gamma\, \varepsilon^{4r} x_3\\ A_{3,r} &= \alpha\beta\, \varepsilon^{r+2} x_1 + \alpha\gamma\, \varepsilon^{2r} x_2 + \beta\gamma\, \varepsilon^{4r+3} x_3,\end{aligned} \tag{7}$$

aus denen leicht zu ersehen ist, dass die 21 Hauptaxen wirklich alle von einander verschieden sind.

Wir fassen dies so zusammen:

2. Es gehören 21 verschiedene Hauptaxen zu der Gruppe G_{168}, von denen jede in jede andere durch Substitutionen der Gruppe transformirt werden kann.

Da es nur 21 Hauptaxen giebt, so muss jede von ihnen durch acht Substitutionen ungeändert bleiben, und diese acht Substitutionen bilden eine Gruppe. Um diese Gruppe zu ermitteln, wenden wir auf den in (6) dargestellten Ausdruck A die Substitution ω [§. 115, (5)] an, und dadurch geht er über in

$$\begin{aligned}\gamma(\alpha^2 + \beta^2\, \varepsilon^3 + \alpha\beta\, \varepsilon^2)\, x_1 + \beta(\alpha\gamma + \gamma^2\, \varepsilon^3 + \alpha^2\, \varepsilon^2)\, x_2&\\ + \alpha(\gamma^2 + \beta\gamma\, \varepsilon^3 + \beta^2\, \varepsilon^2)\, x_3&.\end{aligned} \tag{8}$$

Nach §. 115, (14) und (8) ist aber

$$\alpha^2 + \beta^2 \varepsilon^3 + \alpha \beta \varepsilon^2 = \alpha^2 + \beta (\alpha \varepsilon^2 + \beta \varepsilon^3) = \alpha^2 - \beta \gamma = - \alpha,$$

und wenn man die drei Coëfficienten des Ausdrucks (8) in dieser Weise umformt, so ergiebt sich

$$- \alpha \gamma x_1 - \beta \gamma \varepsilon^3 x_2 - \alpha \beta \varepsilon^2 x_3,$$

d. h. A ändert durch Anwendung der Substitution ω sein Vorzeichen, und die Hauptaxe A bleibt also durch die Substitution ω ungeändert.

Da A ausserdem durch die Substitution Θ ungeändert bleibt, weil zwei Pole von Θ auf A liegen, so haben wir die ganze Gruppe 8ten Grades, durch die A ungeändert bleibt, die wir die Gruppe von A nennen und mit G_a bezeichnen, in der Form

(9) $$\omega^u \Theta^v.$$

Unter diesen acht Substitutionen sind nur zwei, nämlich die identische und Θ^2, die alle Punkte der Linie A ungeändert lassen. Bei den anderen bleiben nur je zwei Punkte in Ruhe. Denn berechnet man auf dem hier eingeschlagenen Wege aus §. 115, (5), (16) die Hauptaxen von ω, $\omega \Theta$, $\omega \Theta^2$, $\omega \Theta^3$, so erhält man, in der Bezeichnung (7),

$$A_{2,1},\ A_{3,0},\ A_{3,3},\ A_{2,0},$$

die alle von der Hauptaxe $A_{1,0}$ von Θ^2 verschieden sind.

Die Substitution Θ^2 hat ausser der Hauptaxe A noch einen isolirten Pol, den wir erhalten, wenn wir die Wurzel $\lambda = 1$ der cubischen Gleichung (4) wählen. Dann ergeben sich für die Coordinaten dieses Poles die Gleichungen

$$\begin{aligned} (\beta - 1) x_1 + \gamma \varepsilon^3 x_2 + \alpha \varepsilon^2 x_3 &= 0, \\ \gamma \varepsilon^{-3} x_2 + (\alpha - 1) x_2 + \beta \varepsilon^{-1} x_3 &= 0, \\ \alpha \varepsilon^{-2} x_1 + \beta \varepsilon x_2 + (\gamma - 1) x_3 &= 0, \end{aligned}$$

und daraus erhält man

(10) $$x_1 : x_2 : x_3 = \alpha \gamma \varepsilon^4 : \beta \gamma \varepsilon : \alpha \beta \varepsilon^2.$$

Solcher Punkte giebt es 21. Den Punkt (10) bezeichnen wir für den Augenblick mit a. Der Punkt a bleibt nun nicht nur durch Θ, sondern auch, wie eine Rechnung auf Grund der Formeln §. 115, (17), (14) zeigt, durch ω, und folglich durch die ganze Gruppe G_a ungeändert, und ist also ein mindestens achtzähliger Pol. Da er aber durch 21 Substitutionen in 21 verschiedene Lagen gebracht werden kann, so ist er auch nicht mehr als

achtzählig. Da er durch die Substitutionen 2ten Grades ω, $\Theta\omega$, $\Theta^2\omega$, $\Theta^3\omega$ ungeändert bleibt, und da die Pole dieser Substitutionen auf A liegen (weil A durch sie ungeändert bleibt), während a nicht auf A liegt, so müssen die Hauptaxen dieser vier Substitutionen ω, $\Theta\omega$, $\Theta^2\omega$, $\Theta^3\omega$ durch den Punkt a gehen.

Die Pole der vier Substitutionen ω, $\Theta\omega$, $\Theta^2\omega$, $\Theta^3\omega$, die wir a_1, a_2, a_3, a_4 nennen wollen, sind als Bilder des Punktes a gleichfalls achtzählige Pole, und müssen, wie a, Pole von Substitutionen vierter Ordnung sein, die jedenfalls alle von Θ und Θ^3 verschieden sind, weil sonst Θ^2 einer jener vier Substitutionen gleich sein müsste, was nicht der Fall ist. Durch ω bleiben nur zwei Punkte der Axe A, nämlich die Pole von ω und von $\Theta^2\omega$, ungeändert.

Betrachten wir nun die beiden anderen Pole c_1, c_2 der Substitution Θ. Diese Punkte liegen gleichfalls auf der Hauptaxe A, sind aber von den Punkten a_1, a_2, a_3, a_4 verschieden, weil diese, wie schon bemerkt, nicht unter den Polen von Θ vorkommen. Nun ist $\omega\Theta\omega = \Theta$, also

$$\omega\,\Theta(x) = \Theta\,\omega(x),$$

und wenn nun $(x) = \Theta(x)$ ist, so ist auch

$$\omega(x) = \Theta\,\omega(x);$$

d. h. wenn (x) die Coordinaten eines Poles von Θ sind, so haben die $\omega(x)$ die gleiche Bedeutung. Durch die Transformation ω gehen also die Pole von Θ nur in einander über. Der Pol a bleibt ungeändert durch ω; c_1 und c_2 dagegen können nicht ungeändert bleiben, weil sie unter den Polen von ω nicht vorkommen, und müssen also in einander übergehen.

Wir haben also folgende Uebersicht:

Ungeändert durch	ω und	$\Theta^2\omega$	auf A	nur	die	Punkte	a_1, a_3
„ „	$\Theta\omega$ „	$\Theta^3\omega$	„ A	„	„	„	a_2, a_4
„ „	Θ „	Θ^3	„ A	„	„	„	c_1, c_2.

Ein von diesen sechs verschiedener Punkt x von A geht nur durch die Substitutionen 1 und Θ^2 in sich selbst über und kann daher ein zweizähliger Pol genannt werden. Dann gilt der Satz:

3. Ein zweizähliger Pol geht durch die aus ω und Θ abgeleitete Gruppe 8ten Grades in vier verschiedene Lagen über.

Ist nämlich x ein zweizähliger Pol, und geht x durch ω in x', durch Θ in x'' über, so sind nicht nur x' und x'' von x, sondern sie sind auch unter einander verschieden, weil, wenn sie identisch wären, x durch $\omega\Theta^3$ ungeändert bliebe. Durch $\omega\Theta$ geht dann x in eine vierte Lage x''' über, und x''' ist sowohl von x' als von x'' verschieden, weil sonst x durch $\omega\Theta\omega = \Theta$ oder durch $\omega\Theta\Theta^{-1} = \omega$ ungeändert bliebe. Da x durch Θ^2 ungeändert bleibt, so geht x durch Θ^3 in x'', durch $\Theta^2\omega = \omega\Theta^2$ in x', durch $\omega\Theta^3$ in x''' über.

Da wir auf jeder Hauptaxe zwei Punkte c_1, c_2 haben, so giebt es im Ganzen 42, und jeder von ihnen kann in jeden anderen durch Substitutionen der Gruppe übergeführt werden. Daraus folgt, dass diese Pole nicht mehr als vierzählig sind. Daher der Satz:

4. Es giebt 21 achtzählige und 42 vierzählige Pole. Auf jeder Hauptaxe liegen vier achtzählige und zwei vierzählige Pole. Durch jeden achtzähligen Pol gehen vier Hauptaxen. Jeder achtzählige Pol kann in jeden anderen achtzähligen und jeder vierzählige Pol in jeden anderen vierzähligen Pol übergeführt werden.

§. 119.

Die drei- und sechszähligen Pole.

Wir wenden uns nun zur Betrachtung der Substitutionen dritter Ordnung und ihrer Pole, und wählen als Repräsentanten einer solchen Substitution

$$\chi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

deren Pole man aus

$$\lambda x_1 = x_3, \quad \lambda x_2 = x_1, \quad \lambda x_3 = x_2$$

erhält. Es folgt daraus $\lambda^3 = 1$; also ist λ eine dritte Einheitswurzel, und wenn daher ϱ eine imaginäre dritte Einheitswurzel bedeutet, so ergeben sich die drei Pole:

$$(1) \qquad \begin{aligned} x_1 &= x_2 = x_3 \\ x_1 &= \varrho\, x_2 = \varrho^2 x_3 \\ x_1 &= \varrho^2 x_2 = \varrho\, x_3. \end{aligned}$$

Zwischen diesen drei Polen besteht aber ein wesentlicher Unterschied. Wenden wir nämlich die Substitution ω darauf an, so bleibt der erste von ihnen ungeändert. Er ist also mindestens sechszählig und gehört zu den Substitutionen

$$1,\ \chi,\ \chi^2,\ \omega,\ \omega\chi,\ \omega\chi^2.$$

Die beiden anderen Pole, nämlich

(2) $$x_1 = \varrho\, x_2 = \varrho^2 x_3,\quad x_1 = \varrho^2 x_2 = \varrho\, x_3,$$

gehen durch die Substitution ω in einander über, und wir müssen nachweisen, dass sie durch jede andere Substitution der Gruppe, ausser χ, χ^2, verändert werden, dass sie also nur dreizählig sind. Bezeichnen wir für den Augenblick die beiden Punkte (2) mit π und π', so können wir zunächst sagen, dass alle Substitutionen aus G_{168}, welche π ungeändert lassen, eine Gruppe G_π bilden müssen, und zwar einen Theiler von G_{168}; die Gruppe G_π enthält ihrerseits die cyklische Gruppe $1, \chi, \chi^2$.

Ist σ irgend eine Substitution von G_π, so kommt also π unter den Polen von σ vor. Daraus folgt, dass σ weder vom 7ten noch vom 4ten Grade sein kann. Denn die Coordinaten der Pole von diesen zwei Graden sind rationale Functionen von ε, i, während die Coordinaten von π die davon unabhängige Irrationalität ϱ enthalten (Bd. I, §. 134, vergl. den Nachtrag am Ende dieses Bandes). Dass aber σ auch nicht vom 2ten Grade sein kann, ergiebt sich daraus, dass π auf keiner der Hauptaxen liegt. Denn läge es auf einer Hauptaxe, so müsste, weil ϱ nicht rational durch ε ausgedrückt werden kann, wie aus (2) mittelst der Gleichung

$$1 + \varrho + \varrho^2 = 0$$

abzuleiten ist, nach §. 118, (7) eine der 21 Relationen bestehen

$$\begin{aligned} \alpha &= \beta\, \varepsilon^{r+3} &&= \gamma\, \varepsilon^{-2r+1}, \\ \alpha &= \beta\, \varepsilon^{-3r+3} &&= \gamma\, \varepsilon^{-r+1}, \\ \alpha &= \beta\, \varepsilon^{2r+3} &&= \gamma\, \varepsilon^{3r+1}, \end{aligned}$$

von denen offenbar keine möglich ist. Die Gruppe G_π enthält also ausser der identischen nur Substitutionen 3ten Grades, und der Grad von G_π muss eine Potenz von 3 sein. Da aber 168 nicht durch 9 theilbar ist, so muss der Grad von G_π gleich 3 sein. Hieraus folgt:

5. Es giebt 56 dreizählige Pole, die zu je zweien zu derselben Substitution gehören, und sich danach in 28 Paare ordnen. Jeder dieser Pole

kann durch Substitutionen der Gruppe G_{168} in jeden anderen transformirt werden.

Setzen wir

$$(3) \qquad T = x_1 + x_2 + x_3,$$

so ist $T = 0$ die Gleichung der Verbindungslinie der Punkte π, π'. Die Function T bleibt durch χ ungeändert und wechselt durch ω ihr Vorzeichen. Sie geht aber durch die 28 Substitutionen $\Theta^s \tau^r$ in 28 verschiedene Functionen $T_{s,r}$ über, die wir mit Hülfe der Formeln des §. 115, (11), (14) leicht so darstellen können:

$$(4) \qquad \begin{aligned} T_{0,r} &= \varepsilon^r x_1 + \varepsilon^{2r} x_2 + \varepsilon^{4r} x_3 \\ h\,T_{1,r} &= \beta^2 \varepsilon^{1+r} x_1 + \alpha^2 \varepsilon^{2+2r} x_2 + \gamma^2 \varepsilon^{4+4r} x_3 \\ -h\,T_{2,r} &= \alpha^2 \varepsilon^{2+r} x_1 + \gamma^2 \varepsilon^{4+2r} x_2 + \beta^2 \varepsilon^{1+4r} x_3 \\ h\,T_{3,r} &= \gamma^2 \varepsilon^{4+r} x_1 + \beta^2 \varepsilon^{1+2r} x_2 + \alpha^2 \varepsilon^{2+4r} x_3, \end{aligned}$$

und diese stellen, gleich Null gesetzt, 28 verschiedene gerade Linien dar, die alle aus einer von ihnen durch Substitutionen der Gruppe ableitbar sind.

Auf der Linie T liegen die drei Punkte mit den Coordinaten

$$\begin{aligned} &\alpha\gamma : \beta\gamma : \beta\alpha \\ &\beta\alpha : \alpha\gamma : \beta\gamma \\ &\beta\gamma : \beta\alpha : \alpha\gamma, \end{aligned}$$

die aus (10), §. 118 durch die Substitutionen $\tau^{-4}, \tau^{-4}\chi, \tau^{-4}\chi^2$ hervorgehen und also zu den achtzähligen Polen gehören.

6. Auf jeder Linie T liegen drei achtzählige und zwei dreizählige Pole.

Es bleibt noch der dritte Pol π_0 der Substitution χ mit den Coordinaten

$$x_1 = x_2 = x_3$$

zu untersuchen, von dem wir schon nachgewiesen haben, dass er durch die sechs Substitutionen

$$(5) \qquad 1, \chi, \chi^2, \quad \omega, \omega\chi, \omega\chi^2$$

ungeändert bleibt. Es fragt sich nun, ob dieser Pol nicht mehr als sechszählig ist.

Wenn es ausser (5) noch andere Substitutionen giebt, die den Pol π_0 unverändert lassen, so müssen diese nothwendig vom 2ten Grade sein, da π_0 weder ein vierzähliger noch ein siebenzähliger Pol ist, und weil ferner der Grad der zu π_0 gehörigen Gruppe nicht durch 9 theilbar sein kann.

Nun liegt der Punkt π_0 auf den drei Hauptaxen der Substitutionen 2ten Grades ω, $\omega\chi$, $\omega\chi^2$. Giebt es noch eine weitere Substitution 2ten Grades, durch die π_0 ungeändert bleibt, so muss π_0 auf der Hauptaxe dieser Substitution liegen.

Setzen wir aber in den Gleichungen der Hauptaxen [§. 118, (7)] $x_1 = x_2 = x_3$, so ist jede dieser drei Gleichungen nur für einen Werth von r befriedigt; also kann π_0 nicht auf mehr als dreien der Hauptaxen liegen, und π_0 ist sechszählig.

Daraus der Satz:

7. Es giebt 42 sechszählige Pole, die alle aus einem von ihnen durch Substitutionen der Gruppe ableitbar sind. Durch jeden dieser Pole gehen drei Hauptaxen der Gruppe.

Der Pol π_0 liegt auf keiner der Linien $T_{s,r}$. Dies lässt sich leicht zeigen, wenn man in den Ausdrücken (4) $x_1 = x_2 = x_3$, und dann für α^2, β^2, γ^2 ihre Ausdrücke durch ε setzt. Man sieht dann leicht (mit Anwendung der Irreducibilität der Kreistheilungsgleichung), dass von diesen Ausdrücken keiner verschwindet.

§. 120.

Die Configuration der Gruppe G_{168}.

Die Gesammtheit der geraden Linien und Punkte, die wir in den vorangegangenen Paragraphen betrachtet haben, wollen wir die Configuration der Gruppe G_{168} nennen. Das Wort hat hier dieselbe Bedeutung, in der es in neuerer Zeit in der Geometrie gebraucht wird [1]).

Wir beschreiben diese Configuration im Folgenden etwas näher, ohne etwas Neues hinzuzufügen, nur um die Sätze der letzten Paragraphen anschaulicher und übersichtlicher hervortreten zu lassen.

Wir haben in dieser Configuration:

21 Linien A (die Hauptaxen),
21 Punkte a (die achtzähligen Pole),
28 Linien T,
28 Punkte t (die sechszähligen Pole).

[1]) Der Ausdruck ist von Reye eingeführt: „Geometrie der Lage." Bd. I, 2. Aufl. (1876).

Das ganze System geht durch 168 Substitutionen der Gruppe in sich selbst über.

Auf jeder Linie A liegen vier Punkte a.
Durch jeden Punkt a gehen vier Linien A.
Auf jeder Linie T liegen drei Punkte a.
Durch jeden Punkt t gehen drei Linien A.

Die Punkte a und t bilden zusammen das vollständige System aller Schnittpunkte der Linien A.

Denn 21 gerade Linien schneiden sich in 210 Punkten, und von diesen fallen drei oder sechs zusammen, wenn drei oder vier dieser Linien durch einen Punkt gehen. Es ist aber $210 = 21.6 + 28.3$.

Auf jeder Linie A liegen vier Punkte t.

Denn da durch jeden Punkt t drei Linien A gehen, und auf jeder Linie A gleich viele Punkte t liegen müssen (weil jede Linie A in jede andere transformirbar ist), so ist, wenn x die Anzahl dieser Punkte ist, $x\,.\,21 : 3 = 28$, also $x = 4$. Ebenso schliesst man:

Durch jeden Punkt a gehen vier Linien T.

Keiner der Punkte t liegt auf einer Linie T.

Bezeichnen wir die ν-zähligen Pole mit P_ν, so haben wir also folgende Systeme von Polen:

21 achtzählige Pole P_8,
28 sechszählige „ P_6,
42 vierzählige „ P_4,
56 dreizählige „ P_3,
24 siebenzählige „ P_7,
unendlich viele zweizählige Pole P_2.

Die P_2 sind alle von P_4, P_6, P_8 verschiedene Punkte der Hauptaxen; von den Punkten P_4 liegen je zwei auf einer Linie A; von den Punkten P_3 liegen je zwei auf einer Linie T; die Punkte P_7 liegen nicht auf den Linien A (dass sie auch nicht auf T liegen, wird sich später ergeben).

Das System der Axen ist genau entsprechend dem System der Pole. Jede gerade Linie, die durch einen achtzähligen Pol geht, ist eine Axe (darunter die Hauptaxen, vier Linien T und zwei Verbindungslinien des P_8 mit P_4). Demnach könnte

man die P_8 passend die **Hauptpole** nennen und die durch sie gehenden Axen mit A_8, A_6, A_4, A_2 bezeichnen.

Hervorzuheben sind ferner die 28 Paare von Verbindungslinien eines P_6 mit den beiden zugehörigen P_3, die wir mit A_3 bezeichnen können, und endlich die 24 Verbindungslinien je zweier zusammengehöriger P_7, als deren Repräsentanten die Seiten des Coordinatendreiecks zu betrachten sind, die mit A_7 bezeichnet werden können.

§. 121.

Invariantencurven der Gruppe G_{168}.

Eine Form μ^{ten} Grades $\varphi(x_1, x_2, x_3)$ wird durch die Substitutionen der Gruppe im Allgemeinen in 168 verschiedene Formen übergehen. Bei besonderen Formen von φ kann diese Zahl sich aber verringern, und dann bilden die Substitutionen, durch die φ ungeändert bleibt, eine in G_{168} enthaltene Gruppe G', deren Grad ein Theiler von 168 sein muss. Die Anzahl der Formen, in die φ übergeht, ist der Index des Theilers G', und jede dieser verschiedenen Formen von φ bleibt durch eine mit G' conjugirte Gruppe ungeändert. Die Form φ ist eine absolute Invariante der Gruppe G'.

Die Gleichung $\varphi = 0$ stellt eine auf das Coordinatendreieck x_1, x_2, x_3 bezogene Curve dar, und diese Curve wird eben durch die Substitutionen von G_{168} auf andere Curven abgebildet. Sind die 168 Bildcurven nicht alle von einander verschieden, so bleibt die Curve φ durch die Substitutionen einer Gruppe G' ungeändert oder ändert sich nur um einen constanten Factor, ist also relative Invariante von G'. Eine gerade Linie bleibt nur dann durch andere als die identische Substitution ungeändert, wenn sie zu den im vorigen Paragraphen beschriebenen Axen gehört.

Alle Eigenschaften und Beziehungen zwischen Punkten, Linien und Curven, die durch lineare Transformation unzerstörbar sind (die sogenannten projectiven Eigenschaften der Geometrie), bleiben in den Bildern erhalten. Wenn also z. B. eine gerade Linie Tangente oder Wendetangente oder Doppeltangente einer Curve ist, so stehen alle Bilder der geraden Linie in derselben Beziehung zu den Bildern der Curve. Ebenso wenn ein Punkt

Doppelpunkt, Wendepunkt, Rückkehrpunkt, Berührungspunkt einer Doppeltangente u. s. w. ist.

Unter den Formen φ sind uns nun vor Allem die von Wichtigkeit, die bei der ganzen Gruppe ungeändert bleiben, die Invarianten, deren es hier, da die Gruppe einfach ist, nur absolute giebt (§. 40). Ist $\Phi(x_1, x_2, x_3)$ eine solche Form, so soll die durch die Gleichung $\Phi = 0$ dargestellte Curve eine invariante Curve der Gruppe heissen. Es giebt 168 Abbildungen der Ebene auf sich selbst, bei denen alle Punkte der Curve in Punkte derselben Curve übergehen. Liegt irgend ein Punkt auf dieser Curve, so liegen auch alle seine Bildpunkte darauf.

Im Allgemeinen ist die Zahl der so mit einander verbundenen Punkte der Curve 168, jedenfalls nicht grösser. Ist sie kleiner, so müssen die Punkte Pole sein, und die Anzahl der Bildpunkte ist ein Theiler von 168 (nämlich 24 für die P_7, 21 für die P_8, 28 für die P_6, 42 für die P_4, 56 für die P_3 und 84 für ein System zusammengehöriger P_2). Wenn ein Pol von einer dieser Arten auf der Curve liegt, so liegen alle Pole von derselben Art darauf.

§. 122.

Die erste Invariante der Gruppe G_{168} und die Grundcurve.

Um nun die Invarianten unserer Gruppe zu bilden, suchen wir Formen der drei Variablen x_1, x_2, x_3 auf, die durch Anwendung der drei Substitutionen χ, τ, ω (§. 115) ungeändert bleiben. Dies genügt, da die ganze Gruppe sich aus diesen drei Substitutionen zusammensetzen lässt (§. 72). Nun ist χ eine cyklische Vertauschung der drei Variablen x_1, x_2, x_3, und τ bedeutet die Substitution

$$\begin{pmatrix} x_1, & x_2, & x_3 \\ \varepsilon x_1, & \varepsilon^2 x_2, & \varepsilon^4 x_3 \end{pmatrix}.$$

Wenn also in einer Invariante ein Glied $x_1^{h_1} x_2^{h_2} x_3^{h_3}$ vorkommt, worin h_1, h_2, h_3 ganze nicht negative Zahlen sind, so verlangt die Unveränderlichkeit durch τ, dass

$$(1) \qquad h_1 + 2h_2 + 4h_3 \equiv 0 \pmod 7)$$

und die Unveränderlichkeit durch χ, dass neben diesem einen Gliede noch die zwei entsprechenden

$$x_2^{h_1} x_3^{h_2} x_1^{h_3}, \quad x_3^{h_1} x_1^{h_2} x_2^{h_3}$$

in der Function vorkommen, wenn nicht $h_1 = h_2 = h_3$ ist. Dazu kommt noch die Bedingung der Unveränderlichkeit durch ω. Wir wollen nun sehen, wie wir diesen Forderungen genügen können, und zwar zunächst so, dass der Grad m der Invariante, d. h. die Summe $h_1 + h_2 + h_3$, möglichst klein wird.

Die Bedingung (1) kann offenbar nicht erfüllt sein, wenn $m < 3$ ist. Ist diese Summe $= 3$, so muss $h_1 = h_2 = h_3 = 1$ sein; aber das Product $x_1 x_2 x_3$ ist offenbar nicht unverändert durch ω. Der kleinste Werth, der in Betracht kommt, ist also $m = 4$, und es sind also alle nicht negativen Lösungen von

$$h_1 + h_2 + h_3 = 4$$
$$h_1 + 2h_2 + 4h_3 \equiv 0 \pmod 7$$

aufzusuchen. Eliminiren wir h_1, so folgt

$$h_2 + 3h_3 \equiv 3 \pmod 7,$$

und daraus ergeben sich die einzig möglichen Lösungen:

$$h_3 = 0, \quad h_2 = 3, \quad h_1 = 1$$
$$h_3 = 1, \quad h_2 = 0, \quad h_1 = 3$$
$$h_3 = 3, \quad h_2 = 1, \quad h_1 = 0,$$

und folglich die einzige, durch χ und τ ungeänderte Form 4ten Grades

(2) $$f(x_1, x_2, x_3) = x_1^3 x_3 + x_2^3 x_1 + x_3^3 x_2.$$

Um den Einfluss der Substitution ω auf die Function f zu prüfen, setzen wir

(3) $$\begin{aligned} x_1 &= \alpha y_1 + \beta y_2 + \gamma y_3 \\ x_2 &= \beta y_1 + \gamma y_2 + \alpha y_3 \\ x_3 &= \gamma y_1 + \alpha y_2 + \beta y_3, \end{aligned}$$

worin die Coëfficienten α, β, γ die in §. 115 festgesetzte Bedeutung haben, und nehmen an, dass durch (3) die Transformation

(4) $$F(y_1, y_2, y_3) = f(x_1, x_2, x_3)$$

geleistet werde. Wir bilden die zweiten Ableitungen von F nach y_1, y_2, y_3 mit Rücksicht auf (3) und auf die Formeln

$$\tfrac{1}{6} f''(x_1, x_1) = x_1 x_3, \quad \tfrac{1}{6} f''(x_2, x_2) = x_2 x_1, \quad \tfrac{1}{6} f''(x_3, x_3) = x_3 x_2$$
$$\tfrac{1}{3} f''(x_2, x_3) = x_3^2, \quad \tfrac{1}{3} f''(x_3, x_1) = x_1^2, \quad \tfrac{1}{3} f''(x_1, x_2) = x_2^2.$$

Daraus ergiebt sich:

$$\begin{aligned} {}^1/_6\, F''(y_1, y_1) &= x_1 x_3 \alpha^2 + x_2 x_1 \beta^2 + x_3 x_2 \gamma^2 \\ &\quad + x_3^2 \beta\gamma + x_1^2 \alpha\gamma + x_2^2 \alpha\beta, \\ {}^1/_3\, F''(y_2, y_3) &= 2 x_1 x_3 \beta\gamma + 2 x_2 x_1 \alpha\gamma + 2 x_3 x_2 \alpha\beta \\ &\quad + x_3^2(\beta\gamma + \alpha^2) + x_1^2(\alpha\gamma + \beta^2) + x_2^2(\alpha\beta + \gamma^2). \end{aligned}$$

Da nun die Auflösungen des Systems (3) von derselben Form sind ($y_1 = \alpha x_1 + \beta x_2 + \gamma x_3, \ldots$), so erhält man hieraus:

$$\begin{gathered} {}^1/_6\, F''(y_1, y_1) - y_1 y_3 = \\ x_1 x_3 (\alpha^2 - \alpha\beta - \gamma^2) + x_2 x_1 (\beta^2 - \beta\gamma - \alpha^2) + x_2 x_3 (\gamma^2 - \beta^2 - \alpha\gamma), \\ {}^1/_3\, F''(y_2, y_3) - y_3^2 \quad = \\ x_1^2 (\beta^2 + \alpha\gamma - \gamma^2) + x_2^2 (\gamma^2 + \alpha\beta - \alpha^2) + x_3^2 (\alpha^2 + \beta\gamma - \beta^2). \end{gathered}$$

Die Coëfficienten auf der rechten Seite dieser Gleichungen $(\alpha^2 - \alpha\beta - \gamma^2) \ldots$ ergeben sich aber aus den Werthen von α, β, γ [§. 115, (11)] als verschwindend, und wir erhalten also, wenn wir noch eine cyklische Vertauschung der x, die eine cyklische Vertauschung der y zur Folge hat, anwenden:

$$\begin{aligned} &{}^1/_6\, F''(y_1, y_1) = y_1 y_3, \quad {}^1/_6\, F''(y_2, y_2) = y_2 y_1, \quad {}^1/_6\, F''(y_3, y_3) = y_3 y_2, \\ &{}^1/_3\, F''(y_2, y_3) = y_3^2, \quad {}^1/_3\, F''(y_3, y_1) = y_1^2, \quad {}^1/_3\, F''(y_1, y_2) = y_2^2. \end{aligned}$$

Demnach ergiebt sich nach dem Euler'schen Satze [Bd. I, §. 17, (6)]:

$$F(y_1, y_2, y_3) = y_1^3 y_3 + y_2^3 y_1 + y_3^3 y_2,$$

und damit ist nachgewiesen, dass die Function $f(x_1, x_2, x_3)$ in der That eine Invariante unserer Gruppe G_{168} ist. Es ist, abgesehen von einem willkürlich beizufügenden constanten Factor, die einzige Invariante 4[ten] Grades.

Die Gleichung

(5) $$f(x_1, x_2, x_3) = 0$$

bedeutet, wenn x_1, x_2, x_3 Coordinaten in der Ebene sind, eine Curve vierter Ordnung, die wir die Grundcurve der Gruppe oder die Curve f nennen wollen, und es giebt 168 Abbildungen der Ebene auf sich selbst, bei denen jedem Punkte dieser Curve ein Punkt der Curve entspricht. Wenn ein Punkt auf der Grundcurve liegt, so liegen auch alle seine Bildpunkte darauf. Die Anzahl der verschiedenen Bildpunkte eines Punktes kann nur dann auf eine kleinere Zahl als 168, und zwar immer auf einen Theiler von 168, heruntersinken, wenn der Punkt ein Pol ist.

Die gerade Linie $x_1 = 0$ schneidet die Curve in drei zusammenfallenden Punkten bei $x_3 = 0$ und in einem vierten davon getrennten Punkte $x_2 = 0$. Die Eckpunkte des Coordinatendreiecks sind also **Wendepunkte** der Curve und die Seiten sind die Wendetangenten. Bezeichnen wir die Seiten des Coordinatendreiecks mit 1, 2, 3 und die gegenüberliegenden Ecken durch dieselben Ziffern, so ist die Seite 1 Wendetangente im Punkt 2, die Seite 2 Wendetangente im Punkt 3 und die Seite 3 Wendetangente im Punkt 1.

Wir untersuchen nun die Lage der Pole und Axen in Bezug auf die Grundcurve. Da die Eckpunkte des Coordinatendreiecks zu den siebenzähligen Polen gehören, so schliessen wir zunächst, dass alle siebenzähligen Pole P_7 auf der Grundcurve liegen.

Es sind, wie die Eckpunkte selbst, alles Wendepunkte der Curve, und diese ordnen sich in acht Wendepunktsdreiecke.

Die dreizähligen Pole P_3 liegen gleichfalls auf der Grundcurve; denn setzt man

$$x_2 = \varrho\, x_1, \quad x_3 = \varrho^2 x_1$$

oder

$$x_2 = \varrho^2 x_1, \quad x_3 = \varrho\, x_1,$$

worin ϱ eine cubische Einheitswurzel ist, so reducirt sich $f(x_1, x_2, x_3)$ auf

$$1 + \varrho + \varrho^2 = 0.$$

Um die Schnittpunkte ihrer Verbindungslinie

$$T = x_1 + x_2 + x_3 = 0$$

mit der Grundcurve zu finden, setzt man $x_3 = -x_1 - x_2$, wodurch $f(x_1, x_2, x_3) = 0$ in

$$x_1^3(x_1 + x_2) - x_2^3 x_1 + (x_1 + x_2)^3 x_2 = (x_1^2 + x_1 x_2 + x_2^2)^2 = 0$$

übergeht. Da die linke Seite ein Quadrat ist, so fallen die vier Schnittpunkte zweimal zu zweien zusammen, und es folgt, dass die Linie T eine Doppeltangente der Grundcurve ist.

Die 28 Linien T sind Doppeltangenten der Grundcurve; ihre Berührungspunkte sind die 56 Pole P_3.

Hieraus folgt beiläufig, dass die Punkte P_7 nicht auf den Linien T liegen, da eine Doppeltangente ausser den Berührungspunkten keinen weiteren Schnittpunkt mit der Curve haben kann.

Die sechs- und achtzähligen Pole liegen nicht auf der Grundcurve.

Für die Punkte P_6 ist dies unmittelbar einzusehen, wenn man [nach §. 119, (1)] $x_1 = x_2 = x_3 = 1$ setzt, wodurch $f(x_1, x_2, x_3) = 3$ wird, also nicht verschwindet. Um dasselbe für die P_8 nachzuweisen, setzt man nach §. 118 (10):

$$x_1 = \alpha\gamma\varepsilon^4, \quad x_2 = \beta\gamma\varepsilon, \quad x_3 = \alpha\beta\varepsilon^2,$$

wodurch, da $\alpha\beta\gamma = \frac{1}{7}$ ist [§. 115, (14)],

$$f(x_1, x_2, x_3) = \tfrac{1}{7}(\alpha^3\gamma^2 + \beta^3\alpha^2 + \gamma^3\beta^2)$$

wird. Setzt man darin [nach §. 115, (8)]:

$$\alpha^3 = \alpha\beta\gamma - \alpha^2, \quad \beta^3 = \alpha\beta\gamma - \beta^2, \quad \gamma^3 = \alpha\beta\gamma - \gamma^2,$$

so erhält man

$$(6)\quad f(x_1, x_2, x_3) = \tfrac{1}{7}\alpha\beta\gamma(\alpha^2 + \beta^2 + \gamma^2) - \tfrac{1}{7}(\alpha^2\gamma^2 + \beta^2\alpha^2 + \gamma^2\beta^2).$$

Aus §. 115, (6), (7) aber folgt

$$\alpha^2 + \beta^2 + \gamma^2 = 1,$$
$$\alpha^2\gamma^2 + \beta^2\alpha^2 + \gamma^2\beta^2 = -\alpha\beta\gamma(\alpha + \beta + \gamma) = \tfrac{1}{7},$$

und daher ist

$$f(x_1, x_2, x_3) = \tfrac{1}{42}$$

von Null verschieden.

Die sämmtlichen Schnittpunkte der 21 Hauptaxen unter einander sind die Pole P_6 und P_8, und folglich schneiden sich niemals zwei Hauptaxen auf der Grundcurve. Die Schnittpunkte der Hauptaxen mit der Grundcurve können also nur vierzählige oder zweizählige Pole sein. Um darüber zu entscheiden, stellen wir folgende Erwägung an. Wenn unter den Schnittpunkten der Hauptaxe A mit der Grundcurve ein P_2 vorkommt, so sind alle vier Schnittpunkte von einander verschieden und sind alle zweizählige Pole. Wenn aber ein P_4 auf A und f liegt, so liegt auch der zweite auf A liegende P_4 auf f, und es kann keinen anderen Schnittpunkt von A und f geben, weil ein solcher ein P_2 wäre und vier weitere P_2 zur Folge hätte. Die vier Schnittpunkte von A und f müssen also paarweise zusammenfallen und A ist eine Doppeltangente. Nun haben wir aber gesehen, dass die 28 Linien T Doppeltangenten sind, und eine Curve vierter Ordnung kann nicht mehr als 28 Doppeltangenten haben. Daher ist die Annahme unzulässig, und es folgt, dass die Schnittpunkte der Grundcurve mit den Hauptaxen zweizählige Pole sind.

Bezeichnen wir also die besonderen zweizähligen Pole, die auf der Curve f liegen, mit $\overline{P}_2$, so haben wir folgende ausgezeichnete Punktsysteme:

$$24\,P_7,\quad 56\,P_3,\quad 84\,\overline{P}_2 \text{ auf der Curve } f.$$
$$21\,P_8,\quad 42\,P_4,\quad 28\,P_6 \text{ nicht auf der Curve } f.$$

Alle anderen Punkte der Curve f gehen durch die Substitutionen der Gruppe in 168 verschiedene Punkte über.

Daraus geht noch unmittelbar hervor, dass die Curve f keinen Doppelpunkt haben und also um so weniger in Curven niedrigeren Grades zerfallen kann. Denn angenommen, sie hätte einen Doppelpunkt, so müssten auch alle seine Bildpunkte Doppelpunkte sein, und weil eine Curve vierter Ordnung, auch wenn sie zerfällt, nicht mehr als sechs Doppelpunkte haben kann, wenn sie nicht unendlich viele Doppelpunkte, d. h. doppelt gezählte Curventheile hat, so müsste f das Quadrat einer quadratischen Form sein. Die Wurzel aus f müsste dann auch eine Invariante sein, während es doch keine quadratischen Invarianten giebt.

Man kann übrigens auch leicht direct zeigen, dass die Grundcurve keinen Doppelpunkt hat; denn die Bedingungen für einen Doppelpunkt sind:

$$f'(x_1) = 3\,x_1^2 x_3 + x_2^3 = 0,$$
$$f'(x_2) = 3\,x_2^2 x_1 + x_3^3 = 0,$$
$$f'(x_3) = 3\,x_3^2 x_2 + x_1^3 = 0,$$

und diese Gleichungen können nicht anders erfüllt sein, als wenn x_1, x_2, x_3 verschwinden (§. 86).

Der Kürze wegen wollen wir ein System von Punkten, deren jeder in jeden anderen durch Substitutionen der Gruppe transformirbar ist, ein System verbundener Punkte nennen.

§. 123.

Die höheren Invarianten.

Weitere Invarianten unserer Gruppe lassen sich nach dem Satze 4., §. 40 ableiten, indem wir Covarianten der Form f bilden. Wir fassen die in §. 87 allgemein besprochenen Covarianten ins Auge, und bilden zunächst die Hesse'sche Covariante

$$(1)\qquad \varDelta = \frac{1}{54}\begin{vmatrix} f''(x_1,x_1), & f''(x_1,x_2), & f''(x_1,x_3) \\ f''(x_2,x_1), & f''(x_2,x_2), & f''(x_2,x_3) \\ f''(x_3,x_1), & f''(x_3,x_2), & f''(x_3,x_3) \end{vmatrix},$$

die entwickelt die Form erhält

$$(2) \qquad \Delta = 5\,x_1^2 x_2^2 x_3^2 - x_1 x_3^5 - x_2 x_1^5 - x_3 x_2^5.$$

Auf der Curve Δ liegen also die Ecken des Coordinatendreiecks, und folglich liegen alle siebenzähligen Pole P_7 auf Δ und bilden das vollständige System der Schnittpunkte von f und Δ.

Eine weitere Covariante, und zwar vom 14ten Grade, erhalten wir aus §. 87, (3), nämlich die Determinante:

$$(3) \qquad C = \frac{1}{9} \begin{vmatrix} f''(x_1, x_1), & f''(x_1, x_2), & f''(x_1, x_3), & \Delta'(x_1) \\ f''(x_2, x_1), & f''(x_2, x_2), & f''(x_2, x_3), & \Delta'(x_2) \\ f''(x_3, x_1), & f''(x_3, x_2), & f''(x_3, x_3), & \Delta'(x_3) \\ \Delta'(x_1), & \Delta'(x_2), & \Delta'(x_3), & 0 \end{vmatrix}.$$

Die Determinante C lässt sich aus (3), wenn auch etwas weitläufig, berechnen, und erhält den Ausdruck:

$$(4) \qquad \begin{aligned} C = \Sigma\, x_1^{14} - 34\, x_1 x_2 x_3\, \Sigma\, x_1^{10} x_3 - 250\, x_1 x_2 x_3\, \Sigma\, x_1^8 x_2^3 \\ + 375\, x_1^2 x_2^2 x_3^2\, \Sigma\, x_1^6 x_2^2 + 18\, \Sigma\, x_1^7 x_2^7 \\ - 126\, x_1^3 x_2^3 x_3^3\, \Sigma\, x_1^3 x_2^2, \end{aligned}$$

worin das Zeichen Σ bedeutet, dass die Summe der drei Glieder genommen werden soll, die man aus dem ersten erhält, wenn man x_1, x_2, x_3 cyklisch vertauscht. Es genügt schon die Berechnung des ersten Gliedes x_1^{14}, um zu erkennen, dass die Curve $C = 0$ nicht durch die Ecken des Coordinatendreiecks geht.

Eine vierte Invariante, und zwar vom 21sten Grade, erhalten wir nach §. 87, (6), wenn wir die Functionaldeterminante der drei Formen f, Δ, C bilden:

$$(5) \qquad K = \frac{1}{14} \begin{vmatrix} f'(x_1), & \Delta'(x_1), & C'(x_1) \\ f'(x_2), & \Delta'(x_2), & C'(x_2) \\ f'(x_3), & \Delta'(x_3), & C'(x_3) \end{vmatrix},$$

die gleichfalls hieraus berechnet werden kann. Wir führen hier nur die drei ersten Glieder an, aus denen man sieht, dass auch diese Curve nicht durch die Ecken des Coordinatendreiecks geht

$$(6) \qquad K = x_1^{21} + x_2^{21} + x_3^{21} + \cdots\ ^{1)}.$$

[1] Die vollständig ausgerechneten Ausdrücke finden sich in der Abhandlung von Gordan: „Ueber die typische Darstellung der ternären biquadratischen Form $f = x_1^3 x_2 + x_2^3 x_3 + x_3^3 x_1$" [Mathem. Annalen. Bd. XVII, S. 366 (1880)]. Auch in Klein-Fricke, Modulfunctionen, Bd. I, S. 734.

§. 124.
Das volle Invariantensystem.

Wir können nun nachweisen, dass die Formen f, Δ, C, K ein volles Invariantensystem der Gruppe sind, d. h. dass alle Invarianten der Gruppe als ganze rationale Functionen von diesen vier dargestellt werden können. Wir stützen uns dabei auf das Theorem von Bezout (Bd. I, §. 49), dass zwei Curven von der m^{ten} und n^{ten} Ordnung, die mehr als $m\,n$ Punkte gemeinsam haben, einen gemeinsamen Curventheil haben müssen. Berührungspunkte sind dabei als doppelt oder mehrfach zu zählen. Alle Schnittpunkte zweier Invariantencurven bilden entweder ein verbundenes System, oder sie zerfallen in Systeme verbundener Punkte, und alle Punkte eines solchen Systemes sind gleich oft zu zählen.

Es sei Φ eine Invariante m^{ter} Ordnung, die die Function f nicht als Factor enthält, und unter den Schnittpunkten der Curve Φ und f mögen h_1 mal die Pole P_7, h_2 mal die Pole P_3, h_3 mal die Pole $\overline{P}_2$ vorkommen. Ausserdem sollen noch h_4 Systeme von je 168 verbundenen Punkten vorkommen, von denen auch (bei Berührung) mehrere Systeme in ein mehrfach gezähltes zusammenfallen können. Dann ist die Anzahl aller Schnittpunkte beider Curven

$$4\,m = 24\,h_1 + 56\,h_2 + 84\,h_3 + 168\,h_4,$$

und daher

$$(1) \qquad m = 6\,h_1 + 14\,h_2 + 21\,h_3 + 42\,h_4,$$

worin h_1, h_2, h_3, h_4 nicht negative ganze Zahlen bedeuten, die auch nicht alle verschwinden können. Der kleinste Werth, den m haben kann, ist daher 6, und eine Invariantencurve 6ter Ordnung muss durch die 24 Punkte P_7 gehen, wie wir es von Δ schon nachgewiesen haben. Ist Δ' eine zweite Invariante 6ter Ordnung, die also auch durch die Punkte P_7 gehen muss, so können wir in $\Delta' - a\,\Delta$ die Constante a so bestimmen, dass die Invariantencurve $\Delta' - a\,\Delta = 0$ durch irgend einen 25sten Punkt von f geht. Dann muss aber, wenn $\Delta' - a\,\Delta$ nicht identisch verschwindet, nach dem Bezout'schen Theorem $\Delta' - a\,\Delta$ durch f theilbar sein. Der Quotient wäre eine Invariante zweiter Ordnung, die nicht existirt; folglich muss $\Delta' - a\,\Delta$ identisch Null sein.

Ist $h_1 = 2$, $h_2 = h_3 = h_4 = 0$, so ist $m = 12$. Eine Invariantencurve 12ter Ordnung Φ muss die Curve f in den 24 Punkten P_7 berühren, und wenn wir in $\Phi - a\Delta^2$ die Constante a passend bestimmen, so ergiebt sich, dass diese Function durch f theilbar sein muss. Der Quotient kann, als Invariante 8ter Ordnung, nur von der Form bf^2 sein, und demnach ist Φ von der Form $a\Delta^2 + bf^3$. Ebenso können wir schliessen, dass eine Invariante 18ter Ordnung die Form $a\Delta^3 + b\Delta f^3$ haben muss.

Alle Invarianten 6ter, 12ter, 18ter Ordnung sind also rationale Functionen von Δ und f.

Der nächste Werth, den m nach (1) haben kann, ist $m = 14$. In diesem Falle ist $h_2 = 1$, während h_1, h_3, h_4 gleich Null sind. Es gehen also alle Invarianten 14ter Ordnung durch die 56 Punkte P_3, und diese bilden das vollständige Schnittpunktsystem einer solchen Invariantencurve mit der Grundcurve. Dies gilt auch von der Invariante C. Haben wir eine zweite Invariante 14ter Ordnung C', so können wir wieder, wie oben, die Constante a so bestimmen, dass $C' - aC$ durch f theilbar ist. Der Quotient ist eine Invariante 10ter Ordnung, und daraus folgt, da es ausser $f\Delta$ keine Invariante 10ter Ordnung giebt:

Jede Invariante 14ter Ordnung ist in der Form darstellbar:

$$aC + bf^2\Delta,$$

worin a, b Constanten sind. Umgekehrt ist jeder Ausdruck von dieser Form eine Invariante 14ter Ordnung.

Es kann sodann m nach (1) den Werth 20 haben, nämlich für $h_1 = h_2 = 1$. Eine Invariante 20ster Ordnung muss also durch die Punkte P_7 und P_3 gehen, d. h. durch die 80 Schnittpunkte von f mit ΔC. Daraus können wir ebenso wie vorhin schliessen, dass eine Invariante 20sten Grades in der Form

$$f(a\Delta^2 + bf^3) + cC\Delta$$

darstellbar ist, worin a, b, c beliebige Constanten sind. Eine unabhängige Invariante 20ster Ordnung giebt es nicht.

Nehmen wir nun an, es seien K' und K zwei Invarianten 21ster Ordnung; beide müssen nach (1) durch die 84 Punkte $\overline{P}_2$ gehen, und folglich kann man a so bestimmen, dass $K' - aK$ durch f theilbar wird. Der Quotient wäre eine Invariante

17ten Grades, die nicht existirt, und folglich ist K' mit aK identisch.

Es giebt also, von einem constanten Factor abgesehen, nur eine Invariante 21sten Grades.

Nun ist aber das System der 21 Hauptaxen auch eine Invariante 21sten Grades, und daraus ist zu schliessen:

Die Invariante K zerfällt in 21 lineare Factoren, die, gleich Null gesetzt, die Hauptaxen der Gruppe darstellen.

Wir können sodann eine Invariante 42sten Grades bilden, nämlich

(2) $$\varDelta^7 - k C^3 = Q,$$

worin k eine beliebige Constante ist, und diese Constante lässt sich so bestimmen, dass die Curve Q durch einen beliebig gegebenen Punkt auf f geht, und sie muss dann auch durch alle mit diesem verbundenen Punkte hindurchgehen. Also können wir k in Q so bestimmen, dass die Curve Q aus der Curve f ein beliebig gegebenes System verbundener Punkte ausschneidet.

Ist nun Φ eine beliebige durch f nicht theilbare Invariante, die h_1, h_2, h_3 mal durch die Pole $P_7, P_3, \overline{P}_2$ geht, und ausserdem durch beliebige Systeme $S_1, S_2, \ldots$ verbundener Punkte auf f, die auch theilweise zusammenfallen können, so bilden wir zunächst nach (2) die Formen $Q_1, Q_2, \ldots$, die in den Systemen $S_1, S_2, \ldots$ verschwinden, und dann die Form

$$\Psi = \Phi - a \varDelta^{h_1} C^{h_2} K^{h_3} Q_1 Q_2 \ldots$$

Die Curve Ψ geht für jeden Werth der Constanten a durch die sämmtlichen Schnittpunkte von Φ mit f, und wenn wir also a so bestimmen, dass Ψ durch irgend einen davon verschiedenen Punkt von f geht, so ist Ψ durch f theilbar, also

$$\Phi = a \varDelta^{h_1} C^{h_2} K^{h_3} Q_1 Q_2 \cdots + f \Phi_1.$$

Darin ist nun Φ_1 wieder eine Invariante, aber von niedrigerem Grade als Φ, und durch vollständige Induction ist hiermit der Satz bewiesen:

Jede Invariante der Gruppe lässt sich als ganze rationale Function der vier fundamentalen Invarianten $f, \varDelta, C, K$ darstellen.

Bestimmt man in (2) die Constante k so, dass die Curve Q durch einen der Pole $\overline{P}_2$ geht, so kann sie durch keinen nicht

mit $\overline{P}_2$ verbundenen Punkt der Curve f gehen; denn sie kann nicht durch die Punkte P_7, P_3 gehen, weil in diesen entweder $\varDelta$ oder C verschwindet, sie kann aber auch nicht durch einen Punkt der Grundcurve gehen, der kein Pol ist, weil sie sonst durch die 168 verbundenen Punkte gehen müsste, und nicht durch den Pol $\overline{P}_2$ gehen könnte. Dann kann man aber die Constante h so bestimmen, dass $K^2 - hQ$ durch f theilbar wird.

Der Quotient ist eine Invariante von niedrigerem als dem 42sten, jedenfalls aber von geradem Grade, und wenn wir ihn also durch die fundamentalen Invarianten darstellen, so kann darin K nicht vorkommen. Daraus folgt:

Die Invariante K^2 kann rational durch f, $\varDelta$, C ausgedrückt werden.

Stellen wir nach diesem Satze K^2 in der Form dar:

$$K^2 = \Sigma\, a f^{\nu} \varDelta^{\nu_1} C^{\nu_2}, \tag{3}$$

so können in dieser Summe, in der die a numerische Coëfficienten sind, nur solche Glieder vorkommen, in denen

$$2\nu + 3\nu_1 + 7\nu_2 = 21,$$

und indem wir nun abzählen, welche Werthe von ν, ν_1, ν_2 vorkommen können, erhalten wir das Resultat, dass zwischen den Formen

$$K^2,\ \varDelta^7,\ C^3,\ f\varDelta^4 C,\ f^2\varDelta C^2,\ f^3\varDelta^5,$$
$$f^4\varDelta^2 C,\ f^6\varDelta^3,\ f^7 C,\ f^9\varDelta$$

eine lineare Relation mit numerischen Coëfficienten besteht.

Stellen wir diese Relation in der Form dar:

$$K^2 = \Phi\varDelta + \Psi C, \tag{4}$$

worin Φ, Ψ gleichfalls Invarianten sind, so können wir daraus noch einen geometrischen Schluss ziehen.

Die Curven $\varDelta$ und C schneiden sich sicher nicht auf der Curve f, weil die sämmtlichen Schnittpunkte von $\varDelta$ mit f die P_7, die von C mit f die P_3 sind. Wenn aber $\varDelta$ und $C = 0$ sind, so ist auch $K = 0$, und folglich liegen alle Schnittpunkte von $\varDelta$ und C auf den 21 Hauptaxen der Gruppe[1]).

[1]) Die Relation (3) ist von Gordan durch die Methoden der Invariantentheorie vollständig berechnet (Mathem. Annalen, Bd. XVII, S. 371).

Wir wollen die dort gegebene Formel in den von uns gebrauchten Zeichen hier angeben:

$$K^2 = C^3 - 88 f^2\varDelta C^2 + 16.63 f\varDelta^4 C + 17.64 f^4\varDelta^2 C - 256 f^7 C$$
$$+ 27.64 \varDelta^7 - 128.469 f^3\varDelta^5 + 43.512 f^6\varDelta^3 - 2048 f^9\varDelta.$$

Die Relation (3) lässt sich benutzen, um aus einem Ausdrucke in den Invarianten alle Potenzen von K, mit Ausnahme der ersten, zu eliminiren, und daraus ergiebt sich noch:

Eine Invariante geraden Grades lässt sich rational durch f, Δ, C, eine Invariante ungeraden Grades als Product von K mit einer Invariante geraden Grades darstellen.

Fünfzehnter Abschnitt.

Das Formenproblem der Gruppe G_{168} und die Theorie der Gleichungen siebenten Grades.

---

§. 125.

Die Resolventen des Formenproblems.

Das Formenproblem für die Gruppe G_{168} (§. 43) liefert nach der allgemeinen Theorie zunächst eine Gleichung 168sten Grades, deren Coëfficienten Invarianten sind. Jeder Theiler der Gruppe führt aber zu einer Resolvente niedrigeren Grades, und zwar vom Grade des Index des Theilers.

Wir wollen hier nur die beiden interessantesten Fälle solcher Theiler, nämlich die Octaëdergruppe

(1) $$G_{24} = \chi^\lambda\, \omega^\mu\, \Theta^\nu,$$

und die Gruppe 21sten Grades

(2) $$G_{21} = \tau^\varrho\, \chi^\lambda \quad (\text{§. } 72)$$

betrachten, die uns zu Resolventen 7ten und 8ten Grades führen.

Was zunächst die Resolventen 7ten Grades anlangt, so können wir bei ihrer Bildung von den Hauptaxen der Gruppe ausgehen. Eine Hauptaxe nämlich bleibt durch die Gruppe $\omega^\mu\, \Theta^\nu$ ungeändert, und geht durch die ganze Gruppe G_{24} in drei verschiedene Linien über. Es muss also sieben Tripel von Hauptaxen geben, die durch eine Gleichung 7ten Grades bestimmt werden.

Setzen wir nach §. 118, (7):

(3) $$\begin{aligned} A_1 &= \alpha\gamma x_1 + \gamma\beta\varepsilon^3 x_2 + \alpha\beta\varepsilon^2 x_3 \\ A_2 &= \beta\gamma\varepsilon^3 x_1 + \alpha\beta\varepsilon^2 x_2 + \alpha\gamma x_3 \\ A_3 &= \alpha\beta\varepsilon^2 x_1 + \alpha\gamma x_2 + \beta\gamma\varepsilon^3 x_3, \end{aligned}$$

so sind $A_1 = 0$, $A_2 = 0$, $A_3 = 0$ die Gleichungen von dreien dieser Axen. Durch die Substitution χ gehen A_1, A_2, A_3 cyklisch in einander über. Durch die Substitution Θ erleiden die Functionen A_1, A_2, A_3 folgende Vertauschung:

$$\begin{pmatrix} A_1, & A_2, & A_3 \\ A_1, & -A_3, & A_2 \end{pmatrix},$$

wie eine einfache Rechnung zeigt, wenn man die Substitution Θ wirklich ausführt und die Formeln des §. 115 benutzt.

Um den Gang der Rechnung wenigstens anzudeuten, sei bemerkt, dass A_1 durch die Substitution Θ [§. 115, (10)] in

$$\alpha\,(\gamma^2\varepsilon^2 + \beta\gamma\varepsilon^3 + \beta^2\varepsilon^5)\,x_1 + \gamma\,(\alpha^2\varepsilon^6 + \beta^2 + \alpha\beta\varepsilon^2)\,x_2$$
$$+ \beta\,(\alpha\gamma + \gamma^2\varepsilon + \alpha^2\varepsilon^3)\,x_3$$

übergeht. Es ist aber nach §. 115, (8), (17), (11):

$$\gamma^2\varepsilon^2 + \beta\gamma\varepsilon^3 + \beta^2\varepsilon^5 = \gamma^2\varepsilon^2 + \alpha^2\varepsilon^3 + \beta^2\varepsilon^5 + \alpha\varepsilon^3$$
$$= \alpha\,(\varepsilon^4 + \varepsilon^{-4}) = h\,(\varepsilon - \varepsilon^{-1}) = \gamma,$$

und daher wird der Coëfficient von x_1 gleich $\alpha\gamma$, wie in A_1, und ebenso formt man die übrigen Ausdrücke um. Da sich nun ω aus Θ und χ zusammensetzen lässt (§. 72), so folgt, dass die Grössen A_1^2, A_2^2, A_3^2 durch die Gruppe G_{24} nur unter einander permutirt werden, und dass demnach ihre symmetrischen Functionen Wurzeln von Resolventen 7ten Grades sind.

Die einfachste symmetrische Function dieser Grössen ist die Summe

(4) $$A_1^2 + A_2^2 + A_3^2,$$

und diese wollen wir, mit einem geeigneten numerischen Factor multiplicirt, als die Unbekannte der Resolvente einführen.

Ordnen wir die Summe (4) nach x_1, x_2, x_3, so erhalten wir dafür einen Ausdruck von der Form

$$\lambda\,(x_1^2 + x_2^2 + x_3^2) + \mu\,(x_2 x_3 + x_3 x_1 + x_1 x_2),$$

worin nach (3):

$$\lambda = (\alpha^2\gamma^2\varepsilon^{-1} + \beta^2\gamma^2\varepsilon^{-2} + \alpha^2\beta^2\varepsilon^3)\,\varepsilon$$
$$\mu = 2\,\alpha\beta\gamma\,(\alpha\varepsilon + \beta\varepsilon^{-3} + \gamma\varepsilon^2)\,\varepsilon.$$

Hierbei ist der Factor ε aus der Klammer gezogen, damit der andere Factor durch die Vertauschung von ε und ε^2 ungeändert bleibt, und sich daher rational durch $\sqrt{-7}$ ausdrücken lässt (Bd. I, §. 171).

Nach den Formeln §. 115, (14) ergiebt sich zunächst sehr einfach:

$$\mu = \frac{2\,\varepsilon}{7},$$

und für λ erhält man, wenn man die Werthe §. 115, (11) für α, β, γ einsetzt, und die Formeln §. 115, (12), (13) benutzt:

$$(5) \qquad \lambda = -\,\varepsilon\,\frac{1+\sqrt{-7}}{14}$$

$$\frac{\mu}{\lambda} = -\,\frac{1-\sqrt{-7}}{2}.$$

Setzt man daher

$$A_1^2 + A_2^2 + A_3^2 = \lambda\, z,$$

so ergiebt sich

$$(6) \quad z = x_1^2 + x_2^2 + x_3^2 - \frac{1-\sqrt{-7}}{2}\,(x_2 x_3 + x_3 x_1 + x_1 x_2),$$

und diese Function wollen wir als Wurzel der Resolvente 7ten Grades einführen. Die übrigen Wurzeln erhält man daraus durch die Substitutionen τ^r, so dass sie alle in der gemeinschaftlichen Form

$$(7). \quad z_r = \varepsilon^{2r} x_1^2 + \varepsilon^{4r} x_2^2 + \varepsilon^{r} x_3^2$$
$$-\,\frac{1-\sqrt{-7}}{2}\,(\varepsilon^{-r} x_2 x_3 + \varepsilon^{-2r} x_3 x_1 + \varepsilon^{-4r} x_1 x_2)$$
$$r = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$$

enthalten sind.

Die Coëfficienten der Gleichung 7ten Grades, deren Wurzeln die sieben Grössen z_r sind, sind Invarianten unserer Gruppe, deren Grad sich leicht angeben lässt.

Wenn nämlich a_ν der Coëfficient von $z^{7-\nu}$ in dieser Gleichung ist, nachdem der Coëfficient der siebenten Potenz auf 1 gebracht ist, so ist a_ν eine Invariante $2\,\nu$ten Grades. Es muss also zunächst $a_1 = 0$ sein, weil es keine quadratische Invariante giebt. Die übrigen Coëfficienten sind durch folgende Invarianten-verbindungen linear und homogen ausgedrückt:

(8)

a_2 durch f,
a_3 „ Δ,
a_4 „ f^2,
a_5 „ Δf,
a_6 „ Δ^2, f^3,
a_7 „ C, Δf^2

und es sind also acht numerische Coëfficienten zu berechnen, die sich durch Vergleichung einiger Glieder in den Ausdrücken der a_ν durch die Wurzeln einerseits, durch die Invarianten (§. 123) andererseits finden lassen, und die ausser rationalen Zahlen nur $\sqrt{-7}$ enthalten können.

Wir wollen diese Coëfficienten zunächst nur unter der Voraussetzung berechnen, dass $f = 0$ ist [1]).

Man braucht dann nur die ersten Glieder (mit $x_1^5 x_2$, $x_1^{10} x_2^2$) in den Potenzsummen Σz_r^3 und Σz_r^6 zu berechnen und die Newton'schen Formeln anzuwenden. Der letzte Coëfficient ergiebt sich aus dem einem Gliede x_1^{14} in dem Producte der z_r. Man findet zunächst

$$\Sigma z_r^3 = -3 \cdot 7 \cdot \frac{1-\sqrt{-7}}{2} x_1^5 x_2 \ldots$$

$$\Sigma z_r^6 = \left[6 . 7 + 15 . 7 \left(\frac{1-\sqrt{-7}}{2}\right)^2\right] x_1^{10} x_2^2 \ldots$$

und daraus die gesuchte Resolvente

$$(9) \quad z^7 - 7 \cdot \frac{1-\sqrt{-7}}{2} \Delta z^4 - 7 \cdot \frac{5+\sqrt{-7}}{2} \Delta^2 z - C = 0.$$

Will man diese Gleichung auf eine andere zurückführen, die nur von den Verhältnissen der x_1, x_2, x_3 abhängt, so setzt man

$$(10) \qquad z = \frac{Cu}{\Delta^2}, \quad g = \frac{\Delta^7}{C^3},$$

wodurch man aus (9) eine Gleichung erhält, in der nur noch der eine Parameter g vorkommt, nämlich

$$(11) \quad u^7 - 7 \, \frac{1-\sqrt{-7}}{2} \, g \, u^4 - 7 \, \frac{5+\sqrt{-7}}{2} \, g^2 u - g^2 = 0.$$

Macht man dieselbe Substitution in der allgemeinen Resolvente, in der f nicht $= 0$ gesetzt ist, so hat man noch einen weiteren Parameter

$$(12) \qquad h = \frac{f \Delta^4}{C^2}$$

einzuführen, und die Coëfficienten der Resolvente werden, von

---

[1]) Dieser Fall ist darum von besonderem Interesse, weil er, ähnlich wie die Ikosaëdergleichung, auf die Transformationsgleichungen aus der Theorie der elliptischen Functionen führt.

numerischen Factoren abgesehen, wie sich aus (8) leicht ergiebt, der Reihe nach

$$h,\ g,\ h^2,\ hg,\ (g^2,\ h^3),\ (g^2,\ h^2 g),$$

worin (g^2, h^3), $(g^2, h^2 g)$ lineare homogene Ausdrücke mit numerischen Coëfficienten bedeuten.

Die Rechnung kann ebenso ausgeführt werden, wie in dem obigen speciellen Falle. Zur Vereinfachung kann man $x_3 = 0$ setzen und erhält immer noch Gleichungen genug zur Bestimmung aller Coëfficienten. Man findet so die Coëfficienten der Reihe nach:

$$7\,\frac{1-\sqrt{-7}}{2}\,h,$$

$$-7\,\frac{1-\sqrt{-7}}{2}\,g,$$

$$-7\,(4+\sqrt{-7})\,h^2,$$

$$14\,(2+\sqrt{-7})\,h\,g,$$

$$-7\,\frac{5+\sqrt{-7}}{2}\,g^2 - 7\cdot\frac{7+3\sqrt{-7}}{2}\,h^3,$$

$$-g^2+\frac{167-7\sqrt{-7}}{2}\,g\,h^2.$$

Die Functionen g, h sind gebrochene Invarianten, die nur von den Verhältnissen $x_1 : x_2 : x_3$ abhängen, und wir können jede andere Invariante von derselben Eigenschaft rational durch g, h ausdrücken. Denn stellen wir eine solche Invariante als Quotienten zweier Formen gleichen Grades ohne gemeinsamen Theiler dar, so müssen Zähler und Nenner ganze Invarianten gleichen Grades sein, weil nämlich zwei in einfachster Form dargestellte gebrochene Functionen der Variablen x nur dann einander gleich sein können, wenn Zähler und Nenner einzeln bis auf constante Factoren einander gleich sind. Hier können nun Zähler und Nenner nicht von ungeradem Grade sein, weil sie sonst den gemeinsamen Factor K hätten (§. 126). Also sind Zähler und Nenner rational durch f, C, Δ darstellbar; und wenn ein im Zähler oder im Nenner vorkommendes Glied

(13) $$f^a \Delta^b C^c,$$

und m der Grad von Zähler und Nenner ist, so ist

(14) $$4a + 6b + 14c = m.$$

Setzen wir nun in (13)

$$\varDelta = (g\,C^3)^{\frac{1}{7}}, \quad f = h\,C^2\,(g\,C^3)^{-\frac{4}{7}},$$

so ergiebt sich für den Ausdruck (13) mit Benutzung von (14)

$$g^{b+2c}\,h^a\,C^{\frac{m}{14}}\,g^{-\frac{m}{7}},$$

und im Zähler und Nenner lässt sich der Factor $C^{\frac{m}{14}}\,g^{-\frac{m}{7}}$ heben, so dass alles rational durch g und h ausgedrückt ist.

Ebenso wie g, h hängt auch die Function u nur von dem Verhältniss der Variablen $x_1 : x_2 : x_3$ ab, und es folgt leicht, dass jede andere Function von derselben Eigenschaft, die wie u die Substitutionen der Gruppe G_{24} gestattet, rational durch u, g, h darstellbar ist. Denn eine solche Function lässt sich zunächst nach den allgemeinen Sätzen des §. 43 als rationale Function von u und den Invarianten darstellen, und zwar nur auf eine Weise als ganze Function von u, die den 6ten Grad nicht übersteigt (Bd. I, §. 142). Die Coëfficienten in dieser Darstellung sind Invarianten, und da u nur von den Verhältnissen abhängt, so können auch die Coëfficienten nur von den Verhältnissen abhängen, und sind daher rational durch g, h darstellbar.

§. 126.

Reduction der allgemeinen Resolvente siebenten Grades auf die specielle.

Wir haben im vorigen Paragraphen zwei Formen der Resolvente 7ten Grades des Formenproblems kennen gelernt, von denen die eine, die specielle, für den Fall gilt, dass $f = 0$ ist, d. h. für den Fall, dass der gesuchte Punkt auf der Grundcurve liegt, die allgemeine für den Fall, dass er eine beliebige Lage hat.

Die Grössen u, g, h wollen wir, wenn sie sich auf den Punkt (x) beziehen, mit

(1) $$u_x = \frac{\varDelta^2 z}{C}, \quad g_x = \frac{\varDelta^7}{C^3}, \quad h_x = \frac{f\varDelta^4}{C^2}$$

bezeichnen. Die allgemeine Resolvente soll dann mit

(2) $$R\,(u_x, g_x, h_x) = R_x = 0$$

bezeichnet werden, und die specielle geht daraus hervor, wenn

man $h_x = 0$ setzt. Die Grössen u_x, g_x, h_x hängen nur von den Variablen x_1, x_2, x_3 ab.

Nun lässt sich, wie Klein a. a. O.[1]) bemerkt hat, die Lösung der allgemeinen Resolvente auf die der speciellen zurückführen, wenn man die Wurzel einer biquadratischen Gleichung adjungirt.

Um dies nachzuweisen, führen wir neben dem Punkte (x) einen zweiten Punkt (y) ein und bilden die Polare von f:

$$(3) \qquad f_1(x,y) = y_1 f'(x_1) + y_2 f'(x_2) + y_3 f'(x_3).$$

Wenn wir dann (x) und (y) gleichzeitig derselben Substitution der Gruppe G_{168} unterwerfen, so bleibt die Function $f_1(x,y)$ ungeändert (Bd. I, §. 60). Wir nehmen nun den Punkt (x) beliebig an, verlangen aber von dem Punkte (y), dass er gleichzeitig auf der Grundcurve und auf der Polaren des Punktes (x) liegen soll, dass also gleichzeitig

$$(4) \qquad f(y_1, y_2, y_3) = 0, \quad f_1(x, y) = 0$$

sein soll. Dann entsprechen jedem Punkte x vier Punkte y, und wenn wir für (x) einen mit ihm verbundenen Punkt setzen, so geht jeder dieser vier Punkte (y) gleichfalls in einen verbundenen Punkt über. Die Function h_y ist jetzt $= 0$ und g_y ist eine vierwerthige Function des Punktes (x). Symmetrische Functionen dieser vier Werthe bleiben ungeändert durch die Substitutionen von G_{168}, und folglich ist g_y Wurzel einer biquadratischen Gleichung, deren Coëfficienten rational von den g_x, h_x abhängen. Die Wurzel dieser biquadratischen Gleichung muss adjungirt werden.

Die Function u_y ist Wurzel der speciellen Resolvente

$$(5) \qquad R(u_y, g_y, 0) = R_y = 0.$$

Wir bezeichnen nun die vier zu demselben x gehörigen Punkte y mit y, y', y'', y''' und bilden die symmetrische Function dieser vier Punkte

$$(6) \qquad (t - u_y)(t - u_{y'})(t - u_{y''})(t - u_{y'''}) = \Phi(t)$$

für ein unbestimmtes t. Diese Function bleibt ungeändert bei allen Substitutionen der Gruppe G_{24}, und ist also rational durch u_x, g_x, h_x ausdrückbar.

---

[1]) Mathematische Annalen, Bd. XV, S. 280.

Da, wenn wir uns die Bestimmung von x vorbehalten, die Gleichung (3) jede beliebige gerade Linie darstellen kann, so können wir x so annehmen, dass unter den vier Punkten y, y', y'', y''' keine zwei verbundenen Punkte vorkommen. Setzen wir dann u_y für die unbestimmte Grösse t in (6), so erhalten wir eine rationale Gleichung

$$(7) \qquad \Psi(u_y, u_x, g, h) = 0,$$

und diese Gleichung ist nicht mehr befriedigt, wenn wir für (x) und (y) eine Substitution aus G_{168} machen, durch die u_x geändert und folglich u_y in einen von $u_y, u_{y'}, u_{y''}, u_{y'''}$ verschiedenen Werth übergeführt wird.

Die Gleichung (7) hat also, als Gleichung für u_x betrachtet, nur eine Wurzel mit der allgemeinen Resolvente R_x gemein, und wenn man den grössten gemeinschaftlichen Theiler von R und Ψ aufsucht, so erhält man u_x rational durch u_y, g, h ausgedrückt. Damit ist die allgemeine Resolvente auf die specielle zurückgeführt.

Die Gruppe G_{168} enthält noch einen Theiler 21sten Grades G_{21}, der durch die Substitutionen χ, τ erzeugt wird, und der zu einer Resolvente 8ten Grades Anlass giebt. Als Wurzel dieser Resolvente kann man einfach das Product $x_1 x_2 x_3$ betrachten. Die Coëfficienten dieser Resolvente sind Invarianten, die bis zum 24sten Grade ansteigen. Wir wollen hier auf diese Resolvente nicht näher eingehen.

§. 127.

Permutationsgruppe von sieben Ziffern vom Grade 168.

Da, wie wir gesehen haben, das Formenproblem der ternären Substitutionsgruppe 168sten Grades eine Resolvente 7ten Grades hat, und die Galois'sche Resolvente dieser Gleichung 7ten Grades folglich vom Grade 168 ist, so ergiebt sich daraus, dass in der allgemeinen Permutationsgruppe von sieben Ziffern, deren Grad $1.2.3.4.5.6.7 = 5040 = 168.30$ ist, ein Theiler vom Grade 168 enthalten sein muss. Die Existenz dieses Theilers hat zuerst

Kronecker erkannt[1]), und seine nähere Untersuchung ist für die allgemeine Theorie der Gleichung 7ten Grades von grosser Wichtigkeit.

Wir können diese Permutationsgruppe dadurch erhalten, dass wir die Permutationen aufsuchen, die durch die Substitutionen der Gruppe G_{168} unter den Grössen $z_0, z_1, z_2, z_3, z_4, z_5, z_6$ (§. 125) hervorgerufen werden. Hierbei ist dann in Bezug auf die Zusammensetzung zu beachten, dass, wenn die beiden linearen Substitutionen ξ_1, ξ_2 die Permutationen π_1, π_2 bewirken, die zusammengesetzte Permutation $\pi_1 \pi_2$ durch $\xi_2 \xi_1$ hervorgerufen wird. Denn nach der Definition erhält man $\xi_2 \xi_1 (x)$ dadurch, dass man auf die Variablen (x) zunächst die Substitution ξ_1 und auf das Ergebniss die Substitution ξ_2 anwendet. Ebenso bedeutet $\pi_1 \pi_2$ die Permutation, die sich ergiebt, wenn man auf die sieben Ziffern zuerst π_1 und darauf π_2 anwendet. Wir erhalten so, der Gruppe G_{168} entsprechend, eine Permutationsgruppe 168sten Grades, die wir mit P_{168} bezeichnen, und diese beiden Gruppen sind isomorph.

Da wir τ und ω als erzeugende Elemente der Gruppe G_{168} erkannt haben (§. 72, I.), so genügt es, wenn wir die diesen beiden Substitutionen entsprechenden Permutationen bestimmen, um daraus die ganze Gruppe P_{168} abzuleiten.

Nun geht aber aus der Substitution τ die cyklische Permutation der sieben Ziffern

$$(\tau) \qquad (0, 1, 2, 3, 4, 5, 6)$$

hervor, und der Einfluss von ω ergiebt sich aus der Bemerkung, dass z_0 durch die Substitutionen der Octaëdergruppe $\chi^\lambda \omega^\mu \Theta^\nu$ ungeändert bleibt. Um also die Aenderung von z_r durch ω zu erhalten, haben wir nur den Einfluss von $\omega \tau^r$ auf z_0 zu ermitteln. Dieser Einfluss aber ergiebt sich unmittelbar aus den Formeln §. 72, (15), wonach z. B. $\omega \tau = \tau^2 \chi^2 \omega \Theta^2$ ist, so dass also z_1 in z_2 übergeht u. s. f. Demnach entspricht der Substitution ω die Permutation

$$(\omega) \qquad \begin{pmatrix} 0, 1, 2, 3, 4, 5, 6 \\ 0, 2, 1, 5, 4, 3, 6 \end{pmatrix} = (1, 2)\,(3, 5).$$

Man kann die Gruppe P_{168} durch die Congruenzgruppe ter-

---

[1]) Kronecker, „Ueber Gleichungen 7ten Grades“. Monatsberichte der Berliner Akademie 1858.

närer linearer Substitutionen für den Modul 2 darstellen, die wir im §. 79 untersucht haben[1]).

Wir haben zu diesem Zweck die sieben Grössen durch drei Indices (x_1, x_2, x_3) zu bezeichnen, die nach dem Modul 2 genommen sind und wobei die Combination (0, 0, 0) ausgeschlossen ist. Man erhält so die sieben Grössen

$$(1) \quad (1,0,0), (0,1,0), (0,0,1), (0,1,1), (1,0,1), (1,1,0), (1,1,1),$$

und wenn man die x_1, x_2, x_3 durch die linearen Verbindungen

$$(2) \quad a x_1 + b x_2 + c x_3,\ a_1 x_1 + b_1 x_2 + c_1 x_3,\ a_2 x_1 + b_2 x_2 + c_2 x_3$$

ersetzt, worin die Substitution

$$(3) \qquad \begin{pmatrix} a, & b, & c \\ a_1, & b_1, & c_1 \\ a_2, & b_2, & c_2 \end{pmatrix}$$

nach dem Modul 2 zu nehmen ist, so erhält man die Permutationsgruppe P_{168}.

Wenn wir, wie im §. 79, für τ die Substitution der Congruenzgruppe

$$(4) \qquad \tau = \begin{pmatrix} 1, & 0, & 1 \\ 1, & 0, & 0 \\ 0, & 1, & 0 \end{pmatrix}$$

wählen, so können wir die Grössen z so bezeichnen, dass sie durch Anwendung von τ und seinen Wiederholungen cyklisch in einander übergehen, wobei wir eine beliebige der Grössen (1) für z_0 wählen können, etwa so:

$$(5) \quad z_0 = (1,0,0),\ z_1 = (1,1,0),\ z_2 = (1,1,1),\ z_3 = (0,1,1),$$
$$z_4 = (1,0,1),\ z_5 = (0,1,0),\ z_6 = (0,0,1).$$

Es ist dann ω so zu wählen, dass z_0, z_4, z_6 dadurch ungeändert bleiben und z_1 mit z_2, z_3 mit z_5 vertauscht werden. Dies giebt

$$(6) \qquad \omega = \begin{pmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 1, & 1 \end{pmatrix},$$

und daraus erhält man nach §. 72, (17):

$$(7) \qquad \chi = \begin{pmatrix} 1, & 0, & 0 \\ 0, & 0, & 1 \\ 0, & 1, & 1 \end{pmatrix}, \quad \Theta = \begin{pmatrix} 1, & 1, & 1 \\ 0, & 1, & 0 \\ 0, & 1, & 1 \end{pmatrix}.$$

---

[1]) Nach einer mündlichen Mittheilung ist dies der Weg, auf dem sie Kronecker gebildet hat.

Die beiden erzeugenden Permutationen τ, ω gehören zur ersten Art (Bd. I, §. 153), und folglich ist P_{168} ein Theiler der alternirenden Permutationsgruppe von sieben Ziffern.

§. 128.

Gleichungen siebenten Grades mit einer Gruppe 168sten Grades.

Wir wenden uns jetzt zu der allgemeinen Theorie der speciellen Art von Gleichungen 7ten Grades, deren Galois'sche Gruppe sich auf P_{168} reducirt.

Es seien zunächst $\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6$ beliebige Grössen, und

(1) $$\tau = (\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6)$$

eine cyklische Permutation 7ten Grades. Führen wir noch das Transpositionspaar

(2) $$\omega = (\lambda_1, \lambda_2)(\lambda_3, \lambda_5)$$

ein, so erzeugen diese beiden Permutationen durch ihre Zusammensetzungen und Wiederholungen die ganze Gruppe P_{168}.

Setzt man nach §. 72, (17) χ und Θ daraus zusammen, so erhält man (da, wie schon oben bemerkt, die Zusammensetzung der Permutationen in umgekehrter Reihenfolge, wie bei den Substitutionen, geschehen muss) die folgenden Permutationen der sieben Indices:

$$\Theta^3 = \tau^6 \omega \tau \omega = (1,2,5,3)(4,6), \quad \Theta = (1,3,5,2)(4,6)$$
$$\chi = \omega \tau^3 \Theta \tau^2 = (1,4,2)(3,5,6),$$

Ausdrücke, die sich auch sehr leicht aus §. 127, (7) ableiten lassen. Man sieht, dass λ_0 durch ω, Θ, χ und folglich durch die ganze in P_{168} enthaltene Octaëdergruppe P_{24} ungeändert bleibt. Es ist leicht, eine Function der sieben Grössen λ zu bilden, die zu der Gruppe P_{168} gehört.

Man nehme z. B. das Product $\lambda_0 \lambda_4 \lambda_6$, das aus den durch ω unberührt bleibenden λ besteht, und bilde die Summe der Producte, die sich daraus durch Anwendung der cyklischen Permutation τ und ihrer Wiederholungen ergeben:

(3) $$v = \lambda_0 \lambda_4 \lambda_6 + \lambda_1 \lambda_5 \lambda_0 + \lambda_2 \lambda_6 \lambda_1 + \lambda_3 \lambda_0 \lambda_2 + \lambda_4 \lambda_1 \lambda_3 + \lambda_5 \lambda_2 \lambda_4 + \lambda_6 \lambda_3 \lambda_5.$$

Wendet man darauf die Substitutionen ω und τ an, so sieht man, dass v ungeändert bleibt und daher alle Permutationen der Gruppe P_{168} gestattet.

Nun ist P_{168} Theiler der symmetrischen Permutationsgruppe von sieben Elementen vom Index 30 und Theiler der alternirenden Gruppe vom Index 15. Folglich ist v Wurzel einer Gleichung 30sten Grades, deren Coëfficienten symmetrische Functionen der λ sind, und Wurzel einer Gleichung 15ten Grades, deren Coëfficienten noch das Differenzenproduct der λ enthalten. Sind die λ die Wurzeln einer Gleichung 7ten Grades ohne Affect, so ist v die Wurzel einer Resolvente 30sten Grades, die durch Adjunction der Quadratwurzel aus der Discriminante in zwei Factoren 15ten Grades zerfällt.

Wenn ausser den symmetrischen Functionen der λ die Grösse v dem Rationalitätsbereiche angehört, sei es, dass sie von vornherein rational ist, oder dass der Rationalitätsbereich durch Adjunction von v erweitert wird, so sind die λ die Wurzeln einer speciellen Gleichung 7ten Grades, deren Galois'sche Gruppe vom 168sten Grade ist. Was wir nun noch zu beweisen haben, ist, dass sich diese specielle Art von Gleichungen 7ten Grades auf das Formenproblem der Gruppe G_{168} zurückführen lässt.

Um dies zu erreichen, müssen wir drei rationale Functionen X_1, X_2, X_3 der Wurzeln λ zu bilden suchen, die, wenn die Permutationen der Gruppe P_{168} ausgeführt werden, die entsprechenden linearen Substitutionen der Gruppe G_{168} erfahren, d. h. die, wenn π eine Permutation aus P_{168} und A die entsprechende Substitution aus G_{168} ist, durch Ausführung der Permutation π in $A\,(X_1, X_2, X_3)$ übergehen.

Setzen wir diese Functionen X_1, X_2, X_3 für die Variablen in die Invarianten der Gruppe G_{168} ein, so gehen diese Invarianten in Functionen der λ_5 über, die durch die Permutationen der Gruppe P_{168} ungeändert bleiben, und die folglich dem Rationalitätsbereiche angehören. Die Berechnung der Werthe der Functionen X_1, X_2, X_3 aus diesen Werthen der Invarianten ist dann das Formenproblem für die G_{168}. Irgend eine durch die Substitutionen von G_{168} veränderte Function der X_1, X_2, X_3 ist Wurzel einer Resolvente der gegebenen Gleichung 7ten Grades, und zwar, da die Gruppen G_{168} und P_{168} einfach sind, eine Totalresolvente.

Hat man irgend ein System nicht verschwindender Functionen X_1, X_2, X_3, so kann man daher solche Resolventen immer bilden. Durch das Formenproblem der Gruppe G_{168} ist also dann die Gleichung 7ten Grades mit der Gruppe P_{168} zugleich gelöst.

Um die Lösung dieser Gleichungen 7ten Grades auf das specielle Formenproblem, wie es bei den elliptischen Functionen auftritt (mit $f = 0$), zurückzuführen, ist dann noch eine accessorische Gleichung 4ten Grades zu lösen, so wie wir, um die allgemeine Gleichung 5ten Grades auf die Ikosaëdergleichung zurückzuführen, eine accessorische Quadratwurzel nöthig fanden.

Alles kommt also jetzt noch darauf an, die Functionen X_1, X_2, X_3 der Wurzeln λ diesen Forderungen gemäss zu bestimmen. Um dies zu ermöglichen, müssen wir einige einfache Sätze aus der allgemeinen Invariantentheorie benutzen, die wir im folgenden Paragraphen, soweit sie für unsere Aufgabe in Betracht kommen, ableiten wollen.

§. 129.

Contragrediente Gruppen.

Wir haben schon im §. 37 den Begriff der contragredienten Transformation erläutert. Sind nämlich

$$(1) \qquad A = \begin{pmatrix} a_1, & b_1, & c_1 \\ a_2, & b_2, & c_2 \\ a_3, & b_3, & c_3 \end{pmatrix}, \quad A_1 = \begin{pmatrix} a_1, & a_2, & a_3 \\ b_1, & b_2, & b_3 \\ c_1, & c_2, & c_3 \end{pmatrix}$$

zwei zu einander transponirte Substitutionen, sind x_1, x_2, x_3 und ξ_1, ξ_2, ξ_3 zwei Reihen von Variablen, die durch die Substitutionen

$$(2) \qquad (y) = A\,(x), \quad \xi = A_1\,(\eta)$$

in zwei neue Reihen von Variablen y_1, y_2, y_3 und η_1, η_2, η_3 transformirt werden, so haben wir diese beiden Reihen von Variablen und ebenso ihre Transformationen contragredient genannt.

Durch die Substitution $y = A\,(x)$ wird jede Function $\Phi\,(x_1, x_2, x_3)$ der (x) in eine Function der (y) transformirt, und die Bildung der Abgeleiteten ergiebt:

$$(3) \qquad \frac{\partial \Phi}{\partial x_1} = a_1 \frac{\partial \Phi}{\partial y_1} + a_2 \frac{\partial \Phi}{\partial y_2} + a_3 \frac{\partial \Phi}{\partial y_3}, \cdots$$

oder in unserer abgekürzten Schreibweise:

$$\left(\frac{\partial \Phi}{\partial x_1}, \frac{\partial \Phi}{\partial x_2}, \frac{\partial \Phi}{\partial x_3}\right) = A_1 \left(\frac{\partial \Phi}{\partial y_1}, \frac{\partial \Phi}{\partial y_2}, \frac{\partial \Phi}{\partial y_3}\right).$$

Dies beweist den Satz:

1. Die Variablenreihen

$$(x_1, x_2, x_3) \text{ und } \left(\frac{\partial \Phi}{\partial x_1}, \frac{\partial \Phi}{\partial x_2}, \frac{\partial \Phi}{\partial x_3}\right)$$

sind contragredient.

Durch wiederholte Anwendung dieses Satzes lassen sich auch die höheren Differentialquotienten nach den x durch die nach den y bilden, wofür man folgende Regel erhält:

2. Um die m^{ten} Ableitungen

$$\frac{\partial^m \Phi}{\partial x_1^\alpha \partial x_2^\beta \partial x_3^\gamma}, \quad \alpha + \beta + \gamma = m$$

durch die Ableitungen nach y auszudrücken, ersetze man in dem entwickelten Ausdrucke

$$(4) \qquad \xi_1^\alpha \xi_2^\beta \xi_3^\gamma = \sum^{\varkappa, \lambda, \mu} C_{\varkappa, \lambda, \mu}^{\alpha, \beta, \gamma} \eta_1^\varkappa \eta_2^\lambda \eta_3^\mu, \quad \varkappa + \lambda + \mu = m$$

die Producte

$$\xi_1^\alpha \xi_2^\beta \xi_3^\gamma \text{ durch } \frac{\partial^m \Phi}{\partial x_1^\alpha \partial x_2^\beta \partial x_3^\gamma}$$

$$\eta_1^\varkappa \eta_2^\lambda \eta_3^\mu \text{ durch } \frac{\partial^m \Phi}{\partial y_1^\varkappa \partial y_2^\lambda \partial y_3^\mu},$$

also

$$(5) \qquad \frac{\partial^m \Phi}{\partial x_1^\alpha \partial x_2^\beta \partial x_3^\gamma} = \sum C_{\varkappa, \lambda, \mu}^{\alpha, \beta, \gamma} \frac{\partial^m \Phi}{\partial y_1^\varkappa \partial y_2^\lambda \partial y_3^\mu},$$

wo unter dem Summenzeichen $\varkappa, \lambda, \mu$ alle nicht negativen der Bedingung $\varkappa + \lambda + \mu = m$ genügenden Werthe durchlaufen.

Die Coëfficienten $C_{\varkappa, \lambda, \mu}^{\alpha, \beta, \gamma}$ sind ganze rationale Functionen der Substitutionscoëfficienten $a_1, a_2, \ldots$

Um diese Regel allgemein zu beweisen, braucht man nur die Formel (5) für $m - 1$ statt m als bewiesen anzusehen, und mit Anwendung der Formel (3) die Ableitung nach einer der Variablen x zu bilden, und dabei die aus der Definition (4) folgende Relation

$$C_{\varkappa, \lambda, \mu}^{\alpha, \beta, \gamma} = C_{\varkappa-1, \lambda, \mu}^{\alpha-1, \beta, \gamma} a_1 + C_{\varkappa, \lambda-1, \mu}^{\alpha-1, \beta, \gamma} a_2 + C_{\varkappa, \lambda, \mu-1}^{\alpha-1, \beta, \gamma} a_3$$

zu berücksichtigen.

Diesen Satz können wir nun auch in folgender Weise verallgemeinern:

3. **Wenn durch die Substitution $y = A(x)$ irgend eine Form $\varphi(x)$ in $\Phi(y)$ übergeht, wenn irgend eine zweite Form $\psi(\xi)$ durch die transponirte Substitution $\xi = A_1(\eta)$ in $\Psi(\eta)$ übergeht, so erhält man eine neue Transformation durch A, wenn man in $\psi(\xi)$ und $\Psi(\eta)$ die Vertauschungen macht**
$$\xi_1^\alpha\, \xi_2^\beta\, \xi_3^\gamma \quad \text{mit} \quad \frac{\partial^{\alpha+\beta+\gamma}\varphi}{\partial x_1^\alpha\, \partial x_2^\beta\, \partial x_3^\gamma}$$
$$\eta_1^\alpha\, \eta_2^\beta\, \eta_3^\gamma \quad \text{mit} \quad \frac{\partial^{\alpha+\beta+\gamma}\Phi}{\partial y_1^\alpha\, \partial y_2^\beta\, \partial y_3^\gamma},$$
wenn man also, wie man sich auch ausdrücken kann, in ψ und Ψ die Potenzen und Producte der Variablen ξ, η durch die entsprechenden Ableitungen von φ, Φ nach den Variablen x, y setzt.

Aus der Compositionsregel der linearen Substitutionen ergiebt sich nun sofort der folgende Satz:

4. **Durchläuft A eine Gruppe G, so durchläuft die transponirte Substitution A_1 eine Gruppe G_1. Sind A, B zwei Elemente aus G und A_1, B_1 die entsprechenden Elemente aus G_1, so sind AB und $B_1 A_1$ entsprechende Elemente. Die Gruppen G und G_1 werden zu einander contragredient genannt.**

Die beiden Gruppen G und G_1 sind aber nur dann isomorph auf einander bezogen, wenn man dem A_1 nicht das Element A, sondern das Element A^{-1} entsprechen lässt; denn dann entspricht $A_1 B_1$ dem Elemente $A^{-1} B^{-1} = (BA)^{-1}$.

Die Invarianten der Gruppe G_1 heissen **Contravarianten** der Gruppe G. Demnach sind auch die Invarianten von G die Contravarianten von G_1.

Aus (3) ergiebt sich dann der folgende Satz:

5. **Wenn man in einer Contravariante von G die Potenzen und Producte der Variablen durch die entsprechenden Ableitungen einer Invariante ersetzt, so erhält man wieder eine Invariante von G**

Und ebenso:

6. **Wenn man in einer Invariante von G die Potenzen und Producte der Variablen durch die entsprechenden Ableitungen einer Contravariante ersetzt, so ergiebt sich wieder eine Contravariante.**

§. 130.

Lösung der Gleichung siebenten Grades mit der Gruppe P_{168} durch das Formenproblem der Gruppe G_{168}.

Die lineare Substitutionsgruppe G_{168} hat die bemerkenswerthe Eigenschaft, dass sie mit sich selbst contragredient ist. Denn die erzeugenden Substitutionen τ, ω von G_{168} (§. 115) bleiben durch Transposition ungeändert, und wenn man also irgend eine Substitution der Gruppe transponirt, so erhält man eine Substitution, die gleichfalls in der Gruppe vorkommt.

Die Contravarianten von G_{168} sind also (von der Bezeichnung der Variablen abgesehen) mit ihren Invarianten identisch.

Die in der Gruppe G_{168} enthaltene Octaëdergruppe G_{24}, die aus den Substitutionen $\chi^\lambda \omega^\mu \Theta^\nu$ besteht, ist aber von ihrer contragredienten Gruppe verschieden; denn es ist z. B. nach §. 72, (17)

$$\Theta^3 = \omega \tau \omega \tau^6,$$

und die dazu transponirte Substitution

$$\Theta_1^3 = \tau^6 \omega \tau \omega$$

lässt sich nach §. 72, (15) in die Form $\tau \chi^2 \Theta^2$ bringen und ist also nicht in G_{24} enthalten.

Es sei nun η_0 irgend eine zu der Gruppe P_{24} gehörige Function der Grössen $\lambda_0, \lambda_1, \ldots, \lambda_6$ (§. 128), z. B. die Wurzel λ_0 selbst. Durch die cyklischen Permutationen τ^ν gehe η_0 in $\eta_0, \eta_1, \ldots, \eta_6$ über. In den Resolventen

$$(1) \qquad \tilde{\omega}_r = \sum_{0,6}^{\nu} \varepsilon^{\nu r} \eta_\nu \qquad r = 1, 2, \ldots, 6$$

ist dann ein System von Functionen gegeben, die sich durch die Permutationen von P_{168} zwar linear, aber nicht ternär substituiren; da man ja die η_ν selbst linear durch die $\tilde{\omega}_r$ ausdrücken kann.

Ein System von drei Functionen, die sich ternär substituiren, kann man auf folgende Weise bilden [1]).

Wir führen zunächst ein System von Hülfsvariablen x_1, x_2, x_3 ein, die wir den Substitutionen der Gruppe G_{168} unterwerfen, und daraus bilden wir die zur Gruppe G_{24} gehörige Function z_0 mit ihren conjugirten z_r [§. 125, (7)]:

(2) $$z_r = \varepsilon^{2r} x_1^2 + \varepsilon^{4r} x_2^2 + \varepsilon^r x_3^2 - \frac{1 - \sqrt{-7}}{2} (\varepsilon^{-r} x_2 x_3 + \varepsilon^{-2r} x_3 x_1 + \varepsilon^{-4r} x_1 x_2).$$

Hierzu nehmen wir nun eine Function η_0 der Wurzeln λ_r unserer Gleichung 7[ten] Grades, die zu der Gruppe P_{24} gehört, z. B. eine rationale Function von λ_0, und die conjugirten Werthe $\eta_0, \eta_1, \ldots, \eta_6$, und bilden die Summe

(3) $$\psi = \eta_0 z_0 + \eta_1 z_1 + \eta_2 z_2 + \eta_3 z_3 + \eta_4 z_4 + \eta_5 z_5 + \eta_6 z_6,$$

die eine quadratische Function der x ist, deren Coëfficienten von den Wurzeln λ_r abhängen.

Diese Function ψ ändert sich nicht, wenn die Variablen (x) einer Substitution der Gruppe G_{168} und die Wurzeln λ_r gleichzeitig der entsprechenden Permutation aus P_{168} unterworfen werden. Denn durch diese gleichzeitige Operation werden in der Summe (2) nur die Summanden unter einander vertauscht, also die Summe selbst nicht geändert.

Wir können daher ψ als simultane Invariante der Gruppen G_{168} und P_{168} bezeichnen.

Ordnen wir die Function ψ nach den Variablen x_1, x_2, x_3, so ergiebt sich

(4) $$\psi = p_1 x_1^2 + p_2 x_2^2 + p_3 x_3^2 + 2 q_1 x_2 x_3 + 2 q_2 x_3 x_1 + 2 q_3 x_1 x_2,$$

worin zur Abkürzung

(5) $$\begin{aligned} p_1 &= \sum^r \varepsilon^{2r} \eta_r, & q_1 &= -\frac{1 - \sqrt{-7}}{4} \sum^r \varepsilon^{-r} \eta_r \\ p_2 &= \sum^r \varepsilon^{4r} \eta_r, & q_2 &= -\frac{1 - \sqrt{-7}}{4} \sum^r \varepsilon^{-2r} \eta_r \\ p_3 &= \sum^r \varepsilon^{r} \eta_r, & q_3 &= -\frac{1 - \sqrt{-7}}{4} \sum^r \varepsilon^{-4r} \eta_r \end{aligned}$$

---

[1]) F. Klein, „Ueber die Auflösung gewisser Gleichungen vom 7[ten] und 8[ten] Grade". Mathem. Annalen, Bd. XV (1879).

gesetzt ist, so dass also die p, q Functionen der Wurzeln λ_r sind.

Nun wählen wir drei verschiedene Functionen η_0, die den bisher ausgesprochenen Bedingungen genügen, und bezeichnen sie mit $\eta_0, \eta_0', \eta_0''$.

Die aus diesen drei Functionen abgeleiteten Formen ψ seien ψ, ψ', ψ'', und deren Coëfficienten (5) $p_i, q_i; p_i', q_i'; p_i'', q_i''$. Dann ist nicht nur jede der drei Functionen ψ, ψ', ψ'' eine simultane Invariante der Gruppen P_{168}, G_{168}, sondern auch ihre Functionaldeterminante (Bd. I, §. 59):

(6) $$\Psi = \frac{1}{8} \begin{vmatrix} \frac{\partial \psi}{\partial x_1}, & \frac{\partial \psi}{\partial x_2}, & \frac{\partial \psi}{\partial x_3} \\ \frac{\partial \psi'}{\partial x_1}, & \frac{\partial \psi'}{\partial x_2}, & \frac{\partial \psi'}{\partial x_3} \\ \frac{\partial \psi''}{\partial x_1}, & \frac{\partial \psi''}{\partial x_2}, & \frac{\partial \psi''}{\partial x_3} \end{vmatrix}.$$

Die Determinante Ψ ist eine Form 3ten Grades in den Variablen x, die nach der Bezeichnungsweise Bd. I, §. 15, (4) den Ausdruck haben mag:

(7) $$\Psi = \Sigma\, A_{h,i,k}\, x_h\, x_i\, x_k.$$

Die Coëfficienten $A_{h,i,k}$ sind dann Functionen der Wurzeln λ_r, die linear und homogen von jedem der drei Systeme $\eta_r, \eta_r', \eta_r''$ abhängen. Solche Functionen nennt man **trilinear**.

Es bedeute nun ξ_1, ξ_2, ξ_3 ein System zu (x) contragredienter Variablen, so dass die biquadratische Form

(8) $$f(\xi_1, \xi_2, \xi_3) = \xi_1^3\, \xi_3 + \xi_2^3\, \xi_1 + \xi_3^3\, \xi_2$$

eine Contravariante von G_{168} ist. Wenn wir nun in (7)

$$x_h\, x_i\, x_k \quad \text{durch} \quad \frac{1}{6} \frac{\partial^3 f}{\partial \xi_h\, \partial \xi_i\, \partial \xi_k}$$

ersetzen, so erhalten wir eine lineare Form

(9) $$L = \frac{1}{6} \Sigma\, A_{h,i,k} \frac{\partial^3 f}{\partial \xi_h\, \partial \xi_i\, \partial \xi_k} = X_1\, \xi_1 + X_2\, \xi_2 + X_3\, \xi_3,$$

in der die X_1, X_2, X_3 Functionen von λ_r sind, und L bleibt nach dem Satze §. 129, 3. ungeändert, wenn die Wurzeln λ_r durch irgend einer Permutation π der Gruppe P_{168} und gleichzeitig die Variablen (ξ) mit den Variablen (x) durch die entsprechende Substitution contragredient transformirt werden.

Geht nämlich durch π der Coëfficient $A_{h,i,k}$ in $A'_{h,i,k}$ über, so ist vermittelst der Transformation $(y) = A(x)$:

$$\Sigma A'_{h,i,k}\, y_h y_i y_k = \Sigma A_{h,i,k}\, x_h x_i x_k,$$

und vermittelst der Substitution $\xi = A_1(\eta)$ besteht die Identität $f(\xi_1, \xi_2, \xi_3) = f(\eta_1, \eta_2, \eta_3)$. Folglich ergiebt sich nach dem Satze §. 129, 3.:

$$\Sigma A'_{h,i,k} \frac{\partial^3 f}{\partial \eta_h \partial \eta_i \partial \eta_k} = \Sigma A_{h,i,k} \frac{\partial^3 f}{\partial \xi_h \partial \xi_i \partial \xi_k}.$$

Bedeutet also π irgend eine Permutation der Gruppe P_{168}, durch die X_1, X_2, X_3 in Y_1, Y_2, Y_3 übergeht, und

$$A = \begin{pmatrix} a_1, & b_1, & c_1 \\ a_2, & b_2, & c_2 \\ a_3, & b_3, & c_3 \end{pmatrix}$$

die entsprechende Substitution aus der Gruppe G_{168}, so haben wir zu setzen:

$$\begin{aligned} \xi_1 &= a_1 \eta_1 + a_2 \eta_2 + a_3 \eta_3 \\ \xi_2 &= b_1 \eta_1 + b_2 \eta_2 + b_3 \eta_3 \\ \xi_3 &= c_1 \eta_1 + c_2 \eta_2 + c_3 \eta_3, \end{aligned}$$

und die Invarianteneigenschaft von L giebt die Relation

$$(10) \qquad Y_1 \eta_1 + Y_2 \eta_2 + Y_3 \eta_3 = X_1 \xi_1 + X_2 \xi_2 + X_3 \xi_3,$$

oder entwickelt

$$(11) \qquad \begin{aligned} Y_1 &= a_1 X_1 + b_1 X_2 + c_1 X_3 \\ Y_2 &= a_2 X_1 + b_2 X_2 + c_2 X_3 \\ Y_3 &= a_3 X_1 + b_3 X_2 + c_3 X_3, \end{aligned}$$

d. h. die Permutation π, auf die Functionen X_1, X_2, X_3 angewandt, hat denselben Erfolg, wie die lineare Substitution $A(X_1, X_2, X_3)$, und demnach sind die X_1, X_2, X_3 solche Functionen, wie sie unser Problem verlangt (Schluss des §. 128).

§. 131.

Möglichkeit der Bestimmung der Functionen X_1, X_2, X_3.

Um die Zurückführung der Gleichung 7ten Grades mit der Gruppe P_{168} auf das Formenproblem der Gruppe G_{168} vollständig sicher zu stellen, bleibt noch Eines übrig:

Es handelt sich nämlich noch um den Nachweis, dass man über $\eta_0, \eta'_0, \eta''_0$ (§. 130) so verfügen kann, dass die Functionen X_1, X_2, X_3 nicht identisch verschwinden. Dazu müssen wir die Bildungsweise der Grössen X etwas genauer betrachten.

Setzen wir in (9) zufolge (8) (§. 130):

$$\frac{\partial^3 f}{\partial \xi_1^3} = 6\,\xi_3,\quad \frac{\partial^3 f}{\partial \xi_1^2 \xi_2} = 0,\quad \frac{\partial^3 f}{\partial \xi_1^2 \partial \xi_3} = 6\,\xi_1,\quad \frac{\partial^3 f}{\partial \xi_1 \partial \xi_2 \partial \xi_3} = 0, \dots,$$

so ergiebt sich

$$(1)\qquad X_1 = A_{2,2,2} + 3\,A_{1,1,3},\quad X_2 = A_{3,3,3} + 3\,A_{2,2,1},$$
$$X_3 = A_{1,1,1} + 3\,A_{3,3,2}.$$

Nun ist aber ferner nach (4) und (6) (§. 130):

$$\Psi =$$
$$(2)\quad \begin{vmatrix} p_1 x_1 + q_3 x_2 + q_2 x_3, & q_3 x_1 + p_2 x_2 + q_1 x_3, & q_2 x_1 + q_1 x_2 + p_3 x_3 \\ p'_1 x_1 + q'_3 x_2 + q'_2 x_3, & q'_3 x_1 + p'_2 x_2 + q'_1 x_3, & q'_2 x_1 + q'_1 x_2 + p'_3 x_3 \\ p''_1 x_1 + q''_3 x_2 + q''_2 x_3, & q''_3 x_1 + p''_2 x_2 + q''_1 x_3, & q''_2 x_1 + q''_1 x_2 + p''_3 x_3 \end{vmatrix}.$$

Dies lässt sich leicht nach Potenzen und Producten der x ordnen, und wenn wir also die Bezeichnung gebrauchen

$$(p_1, q_3, q_2) = \begin{vmatrix} p_1, & q_3, & q_2 \\ p'_1, & q'_3, & q'_2 \\ p''_1, & q''_3, & q''_2 \end{vmatrix} \dots,$$

so erhält man

$$A_{1,1,1} = (p_1, q_3, q_2),\quad 3\,A_{3,3,2} = (q_3, q_1, p_3) + (q_2, p_2, p_3)$$
$$A_{2,2,2} = (q_3, p_2, q_1),\quad 3\,A_{1,1,3} = (p_1, q_1, q_2) + (p_1, q_3, p_3)$$
$$A_{3,3,3} = (q_2, q_1, p_3),\quad 3\,A_{2,2,1} = (q_3, p_2, q_2) + (p_1, p_2, q_1),$$

und daraus nach (1)

$$X_1 = (q_3, p_2, q_1) + (p_1, q_1, q_2) + (p_1, q_3, p_3)$$
$$(3)\qquad X_2 = (q_2, q_1, p_3) + (q_3, p_2, q_2) + (p_1, p_2, q_1)$$
$$X_3 = (p_1, q_3, q_2) + (q_3, q_1, p_3) + (q_2, p_2, p_3).$$

Diese Functionen X_1, X_2, X_3 sind, wie aus dem oben Bemerkten folgt [§. 130, (5)], trilineare Formen der drei Variablenreihen $\eta_r, \eta'_r, \eta''_r$, deren Coëfficienten rational durch die siebente Einheitswurzel ε ausgedrückt werden können. Die Coëfficienten dieser Formen sind aber gewiss nicht alle gleich Null. Denn nach (3) kann man die Grössen p, q so annehmen, dass X_1, X_2, X_3 nicht gleich Null werden, und die 21 Grössen $\eta_r, \eta'_r, \eta''_r$ lassen sich aus §. 130, (5) so bestimmen, dass die 18 Grössen p, q (und ausserdem die drei Summen $\Sigma\,\eta_r$) beliebig vorgeschriebene Werthe

bekommen. Machen wir dann für die sieben Variablen η_r die Substitution

(4) $$\eta_r = a_0 + a_1 \lambda_r + a_2 \lambda_r^2 + a_3 \lambda_r^3 + a_4 \lambda_r^4 + a_5 \lambda_r^5 + a_6 \lambda_r^6,$$

deren Determinante als das Product aller Differenzen $\lambda_i - \lambda_k$ von Null verschieden ist, und substituiren entsprechend

(5) $$\eta_r = \sum_{0,6}^{s} a_s \lambda_r^s, \quad \eta_r' = \sum_{0,6}^{s} a_s' \lambda_r^s, \quad \eta_r'' = \sum_{0,6}^{s} a_s'' \lambda_r^s,$$

so geht dadurch X_1 in eine trilineare Form der drei Variablenreihen a_s, a_s', a_s'' über, die nicht identisch verschwinden kann, weil ja auch umgekehrt die a_s, a_s', a_s'' durch die η_r, η_r', η_r'' linear ausdrückbar sind. Nun kann man für die Variablen a_s, a_s', a_s'' solche rationale Zahlenwerthe annehmen (Bd. I, §. 143), dass die Functionen X_1, X_2, X_3 von Null verschiedene Werthe annehmen, und dann stellt (5) eine geeignete Annahme für die Functionen η_r, η_r', η_r'' dar [1]).

---

[1]) Vergl. über die hiermit erledigte Frage: Burckhardt, „Ueber einen fundamentalen Satz der Lehre von den endlichen Gruppen linearer Substitutionen". Mathem. Annalen, Bd. 42 (1892).

VIERTES BUCH.

ALGEBRAISCHE ZAHLEN.

Sechzehnter Abschnitt.

Zahlen und Functionale eines algebraischen Körpers.

---

§. 132.

Definition der algebraischen Zahlen.

Eine algebraische Gleichung

$$F(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0,$$

deren Coëfficienten $a_1, a_2, \ldots, a_n$ rationale Zahlen sind, nennen wir der Kürze wegen eine rationale Gleichung. Sie hat, wie wir in früheren Abschnitten nachgewiesen haben, immer n oder weniger, aber immer wenigstens eine Wurzel. Wie man jeder dieser Wurzeln durch rationale Zahlen, etwa durch Decimalbrüche oder durch Kettenbrüche, nöthigenfalls mit Zuziehung der imaginären Einheit $i = \sqrt{-1}$ bis auf jeden beliebigen Grad nahe kommen kann, d. h. wie man die Werthe der Wurzeln annähernd berechnen kann, ist im zweiten Buche des ersten Bandes gezeigt.

In den folgenden Betrachtungen soll es sich nun nicht um diese numerischen Werthe handeln, sondern um die arithmetischen Gesetze, denen diese Zahlen unterworfen sind, die sich aus der Definition selbst und nicht aus den numerischen Werthen ableiten lassen. Wir stellen also jetzt folgende Definition an die Spitze:

Eine Zahl Θ, die einer rationalen Gleichung

(1) $$F(\Theta) = 0$$

genügt, heisst eine algebraische Zahl.

Jede algebraische Gleichung mit rationalen Coëfficienten liefert uns solche algebraische Zahlen, die sich also in beliebiger Menge angeben lassen. Die Frage, ob es auch nicht algebraische Zahlen giebt, wird uns später beschäftigen.

Eine algebraische Zahl genügt nicht nur einer, sondern unendlich vielen rationalen Gleichungen; denn multiplicirt man zwei beliebige Functionen von der Form $F(x)$ mit einander, so erhält man eine Function derselben Form, die für $x = \Theta$ verschwindet, wenn einer der Factoren diese Eigenschaft hat.

Unter allen rationalen Gleichungen, denen eine algebraische Zahl genügt, ist eine von möglichst niedrigem Grade, $f(\Theta) = 0$, wenn $f(x)$ die Form hat:

$$(2) \qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n,$$

und es kann auch nur eine solche Gleichung geben, wenn wir, wie bisher immer, den Coëfficienten der höchsten Potenz von x gleich 1 annehmen.

Denn sind $f(x), f_1(x)$ zwei Functionen von der Form (2) von gleichem Grade n, so ist $f(x) - f_1(x)$ von niedrigerem als dem n^{ten} Grade, und wenn sowohl $f(\Theta)$ als $f_1(\Theta)$ verschwindet, so verschwindet auch $f(\Theta) - f_1(\Theta)$; wenn also diese Differenz nicht identisch verschwindet, so genügt Θ einer Gleichung von niedrigerem als dem n^{ten} Grade, was gegen die Voraussetzung ist.

Die Function $f(x)$ ist im Körper der rationalen Zahlen irreducibel.

Denn zerfällt $f(x)$ in zwei rationale Factoren $f_1(x)$ und $f_2(x)$, von denen jeder von niedrigerem Grade ist als $f(x)$, so genügt Θ einer der beiden Gleichungen $f_1(\Theta) = 0$, $f_2(\Theta) = 0$, was unserer Voraussetzung widerspricht.

Ist n der Grad der rationalen Gleichung niedrigsten Grades, der die Zahl Θ genügt, so nennen wir Θ eine algebraische Zahl n^{ten} Grades.

§. 133.

Ganze algebraische Zahlen.

Eine algebraische Zahl Θ wird eine ganze algebraische Zahl genannt, wenn sie einer rationalen Gleichung

$$(1) \qquad \Theta^m + A_1 \Theta^{m-1} + \cdots + A_{m-1}\Theta + A_m = 0$$

genügt, deren Coëfficienten $A_1, A_2, \ldots, A_m$ ganze Zahlen sind.

Wir bemerken, dass es nach dieser Definition ausreicht, um eine algebraische Zahl Θ als ganz zu charakterisiren, wenn unter den unendlich vielen Gleichungen der Form (1), denen Θ genügt, eine ist, deren Coëfficienten ganze Zahlen sind.

Die ganzen algebraischen Zahlen umfassen als speciellen Fall die gewöhnlichen ganzen Zahlen, die wir zur Unterscheidung ganze rationale Zahlen nennen. Die positiven ganzen rationalen Zahlen nennen wir auch, einem verbreiteten Sprachgebrauch folgend, natürliche Zahlen.

Unter ganzen Zahlen schlechtweg verstehen wir dann ganze algebraische, rationale und irrationale Zahlen.

1. Eine ganze algebraische Zahl, die zugleich rational ist, ist nothwendig eine ganze rationale Zahl.

Nehmen wir nämlich an, es sei $\Theta = P : Q$ ein rationaler Bruch, und P, Q ganze rationale Zahlen ohne gemeinsamen Theiler, etwa Q positiv, so ergiebt sich aus (1)

$$P^m + A_1 P^{m-1} Q + A_2 P^{m-2} Q^2 + \cdots + A_m Q^m = 0,$$

und daraus ist zu ersehen, dass jeder Primtheiler von Q in P enthalten sein müsste. Es muss also $Q = 1$ sein, und $\Theta = P$ ist eine ganze rationale Zahl.

2. Summe, Differenz und Product zweier ganzer Zahlen sind wieder ganze Zahlen.

Um diesen Hauptsatz zu beweisen, nehmen wir an, es seien α, β zwei ganze Zahlen, die den Gleichungen

$$(2) \qquad \begin{aligned} \alpha^\mu + a_1 \alpha^{\mu-1} + \cdots + a_{\mu-1} \alpha + a_\mu &= 0 \\ \beta^\nu + b_1 \beta^{\nu-1} + \cdots + b_{\nu-1} \beta + b_\nu &= 0 \end{aligned}$$

genügen, und machen eine der drei Annahmen

$$\omega = \alpha + \beta, \quad \alpha - \beta, \quad \alpha \beta.$$

Dann setzen wir $\mu \nu = m$ und bezeichnen die m Grössen

$$\alpha^r \beta^s \qquad \begin{aligned} r &= 0, 1, \ldots, \mu - 1 \\ s &= 0, 1, \ldots, \nu - 1 \end{aligned}$$

in irgend einer Reihenfolge mit $\omega_1, \omega_2, \ldots, \omega_m$.

Dann können die Producte $\omega\omega_1, \omega\omega_2, \ldots, \omega\omega_m$ mit Hülfe der Gleichungen (2) in die Form gesetzt werden

$$\omega\omega_r = c_{r,1}\omega_1 + c_{r,2}\omega_2 + \cdots + c_{r,m}\omega_m$$
$$r = 1, 2, \ldots, m,$$

worin die Coëfficienten $c_{s,r}$ ganze rationale Zahlen sind. Wenn man aus diesen Gleichungen aber die $\omega_1, \omega_2, \ldots, \omega_m$ eliminirt, so folgt

$$\begin{vmatrix} c_{1,1}-\omega, & c_{1,2}, & \ldots, & c_{1,m} \\ c_{2,1}, & c_{2,2}-\omega, & \ldots, & c_{2,m} \\ \cdot & \cdot & \cdot & \cdot \\ c_{m,1}, & c_{m,2}, & \ldots, & c_{m,m}-\omega \end{vmatrix} = 0,$$

was entwickelt die Form enthält

$$\omega^m + C_1\omega^{m-1} + \cdots + C_m = 0,$$

worin die $C_1, C_2, \ldots, C_m$ gleichfalls ganze rationale Zahlen sind. Dies aber zeigt, dass ω eine ganze Zahl ist, wie bewiesen werden sollte.

3. Ist $f(x)$ eine im Körper der rationalen Zahlen irreducible Function, und ist eine Wurzel Θ von $f(x) = 0$ eine ganze Zahl, so sind alle Wurzeln von $f(x)$ ganze Zahlen.

Denn wenn eine rationale Function $F(x)$ für $x = \alpha$ verschwindet, so ist $F(x)$ durch $f(x)$ theilbar, und alle Wurzeln von $f(x)$ sind zugleich Wurzeln von $F(x)$ (Bd. I, §. 141). Wenn nun α eine ganze Zahl ist, so giebt es eine Function

$$F(x) = x^m + A_1x^{m-1} + \cdots + A_m$$

mit ganzzahligen Coëfficienten $A_1, \ldots, A_m$, die für $x = \alpha$ verschwindet, und $F(x)$ verschwindet also auch für alle anderen Wurzeln von $f(x)$, die sonach alle ganze Zahlen sind.

Ist

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n,$$

so sind die $a_1, a_2, \ldots, a_n$ durch Multiplication und Addition aus den Wurzeln von $f(x)$ zusammengesetzt und sind also nach 2. ganze rationale Zahlen. Daraus folgt:

4. Ist Θ eine ganze algebraische Zahl, so hat die Gleichung niedrigsten Grades $f(\Theta) = 0$ [§. 132, (2)] ganzzahlige Coëfficienten.

Wir beweisen noch den Satz:

5. **Jede algebraische Zahl Θ lässt sich durch Multiplication mit einer natürlichen Zahl in eine ganze algebraische Zahl verwandeln.**

Denn ist

$$\Theta^m + A_1 \Theta^{m-1} + \cdots + A_m = 0,$$

und sind $A_1, \ldots, A_m$ rationale Zahlen mit dem gemeinsamen Nenner a, so erhält man durch Multiplication mit a^m:

$$(a\Theta)^m + A_1 a (a\Theta)^{m-1} + A_2 a^2 (a\Theta)^{m-2} + \cdots + A_m a^m = 0,$$

woraus hervorgeht, dass $a\Theta$ eine ganze Zahl ist.

§. 134.

Algebraische Körper.

Im dreizehnten Abschnitte des ersten Bandes haben wir gesehen, wie man aus jeder Wurzel Θ einer in irgend einem Körper Ω irreduciblen Gleichung n^{ten} Grades $f(\Theta) = 0$ einen algebraischen Körper $\Omega(\Theta)$ über Ω ableitet. Die aus den n Wurzeln dieser Gleichung abgeleiteten n Körper, die auch zum Theil oder alle identisch sein können, haben wir conjugirte Körper genannt.

Bezeichnen wir mit R den Körper der rationalen Zahlen, so giebt also nach unserer Definition jede algebraische Zahl n^{ten} Grades, Θ, Anlass zu einem algebraischen Körper $R(\Theta)$ über R, den wir von jetzt an kurz einen algebraischen Zahlkörper n^{ten} Grades nennen. Wir haben auch schon früher nachgewiesen (Bd. I, §. 143), dass man immer einen algebraischen Zahlkörper bestimmen kann, der eine endliche Anzahl beliebig gegebener algebraischer Zahlen enthält.

Dieser Satz wird an dieser Stelle hervorgehoben, um darauf hinzuweisen, dass die Allgemeinheit einer Betrachtung über irgend eine endliche Anzahl algebraischer Zahlen dadurch nicht beeinträchtigt wird, dass man diese Zahlen alle in einem algebraischen Zahlkörper gelegen voraussetzt.

Jede Zahl ω eines solchen Körpers kann als ganze Function $\varphi(\Theta)$ von Θ mit rationalen Coëfficienten dargestellt werden, und jeder Zahl ω entspricht in jedem der n conjugirten Körper eine bestimmte Zahl. Diese conjugirten Zahlen können zum Theil einander gleich sein, und wir haben danach primitive und

imprimitive Zahlen des Körpers unterschieden. Eine symmetrische Function der conjugirten Zahlen ist eine rationale Zahl. Unter diesen symmetrischen Functionen sind zwei von besonderer Wichtigkeit, die Summe und das Product, von denen die erste die Spur, die zweite die Norm von ω genannt wird. Man bezeichnet diese beiden Zahlen durch $S(\omega)$ und $N(\omega)$.

Hierbei werden, wenn unter den conjugirten Zahlen dieselben Zahlen mehrfach vorkommen, diese gleichen Zahlen so oft in die Summe oder das Product aufgenommen, als der Grad ihrer Häufigkeit angiebt.

Da sich in jedem solchen Zahlkörper die vier fundamentalen Rechenoperationen ebenso wie im Körper der rationalen Zahlen ausführen lassen, so kann man auch die Frage aufwerfen, inwieweit sich die aus der Theorie der rationalen Zahlen bekannten arithmetischen Grundgesetze in einem beliebigen algebraischen Zahlkörper bewähren. Es handelt sich hierbei in erster Linie um die Zerlegung der ganzen Zahlen in ihre Primfactoren.

Da diese Zerlegung mit den Zahlen des algebraischen Körpers selbst im Allgemeinen nicht gelingt, so ist eine Erweiterung des Rechenmateriales nöthig, um die einfachen Gesetze wieder herzustellen, und eine solche Erweiterung ist in verschiedenem Sinne möglich. Es müssen sich aber diese verschiedenen Erweiterungen auf einander zurückführen, oder, genauer gesagt, in eine eindeutige Beziehung zu einander setzen lassen.

Kummer hat zuerst für die aus Einheitswurzeln gebildeten algebraischen Zahlen (die Kreistheilungszahlen) das grosse Problem durch die Schöpfung der idealen Zahlen [1]) gelöst. Eine andere ganz allgemeine, keiner Ausnahme unterworfene Lösung hat die Aufgabe durch Dedekind gefunden, der als die einfachsten Elemente der Rechnung die von ihm so genannten Ideale [2])

---

1) Kummer, Theorie der idealen Primfactoren der complexen Zahlen etc. Crelle's Journal, Bd. 35, 1846, Bd. 40, 1850. Abhandlungen der Berliner Akademie 1856. Sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers. Liouville's Journal, Bd. 16, 1851.

2) Dedekind, in dem letzten Supplement der 2., 3. und 4. Auflage von Dirichlet's Vorlesungen über Zahlentheorie (Braunschweig 1871, 1879, 1894). Zu vergleichen ist auch: Sur la théorie des nombres entiers algébriques im Bulletin von Darboux und Hoüel (1re sér. XI, 1877). Ueber den Zusammenhang zwischen der Theorie der Ideale und der höheren Congruenzen (Abhandlungen der Ges. der Wissensch. in Göttingen, Bd. 23,

betrachtet. Einen davon verschiedenen Weg hat Kronecker[1] eingeschlagen.

Die Theorie von Dedekind ist von ihrem Begründer umfassend und in stets wachsender Einfachheit und Vollkommenheit dargestellt in dem letzten Supplement der drei neuesten Auflagen von Dirichlet's Vorlesungen über Zahlentheorie.

Die Theorie von Kronecker ist erst im Jahre 1882 durch die Festschrift zu Kummer's Jubiläum dem weiteren Kreise der Mathematiker bekannt geworden, und ist auch jetzt noch nicht ganz leicht zugänglich[2].

Bezüglich der Dedekind'schen Theorie können wir also den Leser, der tiefer in diesen interessanten Gegenstand einzudringen wünscht, auf die genannten Werke verweisen. Dagegen soll hier der Versuch gemacht werden, den Zusammenhang zwischen den verschiedenen Theorieen herzustellen und auf Grund der Kronecker'schen Voraussetzungen und Hülfsmittel so viel daraus zu entwickeln, als für die folgenden algebraischen Anwendungen nothwendig ist.

§. 135.

Ganze Functionen in einem algebraischen Körper.

Schon im ersten Bande haben wir mehrfach Gelegenheit gehabt, ganze Functionen einer beliebigen Anzahl von unabhängigen Veränderlichen einzuführen, und haben auch (in §. 141 f.)

1878). Ueber die Discriminanten endlicher Körper (ebend., Bd. 29, 1882). Ueber die Anzahl der Ideal-Classen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig 1877). Festschrift zur Säcularfeier des Geburtstages von Gauss. „Zur Theorie der Ideale" und „Ueber die Begründung der Idealtheorie". Nachrichten d. Ges. d. Wissensch. in Göttingen 1894, 1895. Hierher gehören auch die Abhandlungen von Hilbert, „Ueber die Zerlegung der Ideale etc.", Mathem. Annalen, Bd. 44, 1893. „Grundzüge einer Theorie der Galois'schen Zahlkörper", Göttinger Nachrichten 1894. Hurwitz, „Zur Theorie der Ideale". „Ueber einen Fundamentalsatz etc.", Göttinger Nachrichten 1894, 1895.

[1]) Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Festschrift zu Kummer's 50jährigem Doctor-Jubiläum. Berlin 1882. (Auch in Bd. 92 von Crelle's Journal.) Zu erwähnen sind hier noch die Arbeiten von Hensel in den Bänden 101, 103, 105, 111, 113 des Crelle'schen Journals.

[2]) Vgl. die Vorrede zur 4. Auflage von Dirichlet-Dedekind's Vorlesungen über Zahlentheorie.

den Fall erörtert, dass die Coëfficienten einem bestimmten Körper Ω angehören. Wir machen jetzt die Annahme, dass dieser Körper Ω ein **algebraischer Zahlkörper** sei, und betrachten also Ausdrücke $\varphi(x, y, z, \ldots)$, die als eine Summe von Gliedern der Form

$$\alpha x^r y^s z^t \ldots$$

dargestellt sind, worin die Exponenten $r, s, t, \ldots$ positive oder wenigstens nicht negative ganze Zahlen sind, während die Coëfficienten α Zahlen in Ω bedeuten. Einen solchen Ausdruck

$$(1) \qquad \varphi(x, y, z, \ldots) = \Sigma\, \alpha x^r y^s z^t \ldots$$

nennen wir eine **ganze Function in Ω**. Wir nehmen den Ausdruck immer so geordnet und zusammengefasst an, dass dieselbe Combination der Exponenten $r, s, t, \ldots$ nicht zweimal darin vorkommt, und nennen zwei solche Ausdrücke nur dann einander gleich, wenn sie dieselben Producte $x^r y^s z^t \ldots$, mit denselben Coëfficienten behaftet, enthalten. **Eine ganze Function wird dann und nur dann gleich Null gesetzt, wenn alle ihre Coëfficienten Null sind.**

Mehrere ganze Functionen geben durch Addition, Subtraction und Multiplication immer wieder ganze Functionen. Nach Bd. I, §. 143, I. kann man für die Variablen $x, y, z, \ldots$ solche rationale Zahlwerthe setzen, dass eine oder eine beliebige Anzahl von gegebenen von Null verschiedenen ganzen Functionen in Ω nicht verschwindende Zahlwerthe (in Ω) erhalten. Daraus ergiebt sich, dass **ein Product mehrerer ganzer Functionen nur dann verschwindet, wenn einer seiner Factoren verschwindet.**

Die Summe $r + s + t + \cdots$ der Exponenten in einem Gliede des Ausdrucks (1) heisst der **Grad dieses Gliedes**, und der grösste Werth, den der Grad eines Gliedes mit nicht verschwindendem Coëfficienten in φ annimmt, heisst der **Grad der Function φ**.

Der Grad eines Productes aus zweien oder mehreren ganzen Functionen ist gleich der Summe der Grade der einzelnen Factoren.

Denn fasst man in jedem der Factoren die Summe der Glieder höchsten Grades zu einer homogenen Function zusammen, so erhält man die Glieder höchsten Grades des Productes, wenn man alle diese homogenen Functionen mit einander multiplicirt

Das Product dieser homogenen Functionen kann nach dem oben Bewiesenen nicht verschwinden, wenn keiner der Factoren verschwindet, und sein Grad ist gleich der Summe der Grade der einzelnen Factoren.

Die Zahlen des Körpers Ω sind unter den Functionen mit enthalten. Man erhält sie, wenn man entweder den Grad oder die Anzahl der Variablen auf Null heruntersinken lässt.

Ueber die ganzen Functionen in Ω haben wir im ersten Bande mehrere wichtige Sätze abgeleitet, von denen wir hier den Satz §. 141, IV hervorheben:

1. Unter den ganzen Functionen in Ω müssen reducible und irreducible unterschieden werden, von denen die ersten als Product aus mehreren ganzen Functionen in Ω darstellbar sind, die anderen nicht. Die reduciblen Functionen φ lassen sich in eine endliche Anzahl von irreduciblen Factoren zerlegen, die selbst ganze Functionen in Ω sind, und die irreduciblen Factoren von φ sind, von constanten Factoren, d. h. Zahlen in Ω, abgesehen, eindeutig durch φ selbst bestimmt.

Als specielle Fälle sind unter den ganzen Functionen in Ω auch die ganzen Functionen im Körper der rationalen Zahlen R enthalten:

$$\Phi(x, y, z, \ldots) = \sum a\, x^r y^s z^t \ldots, \tag{2}$$

worin die Coëfficienten a rationale Zahlen sind.

Wenn diese Coëfficienten ganze Zahlen ohne gemeinsamen Theiler sind, so heisst diese Function eine ursprüngliche oder primitive, von denen wir im Bd. I, §. 2 den Satz nachgewiesen haben:

2. Das Product von zwei primitiven Functionen ist wieder eine primitive Function.

Wenn die Coëfficienten der Function (2), die wir für den Augenblick mit

$$a_0, a_1, a_2, \ldots$$

bezeichnen wollen, ganze Zahlen mit dem grössten gemeinschaftlichen Theiler m sind, so ist, wenn $m > 1$ ist, Φ eine imprimitive ganze ganzzahlige Function vom Theiler m, und der Theiler einer primitiven Function ist $= 1$.

Setzen wir

(3) $a_0 = m e_0,\ a_1 = m e_1,\ a_2 = m e_2 \ldots,$

so sind die $e_0, e_1, e_2, \ldots$ ganze Zahlen ohne gemeinsamen Theiler;

(4) $E(x, y, z, \ldots) = \sum e x^r y^s z^t \ldots$

ist eine primitive Function und es wird

$$\Phi = m E.$$

Diese Functionen Φ haben wir im §. 2 des ersten Bandes betrachtet und haben dort von ihnen den Satz bewiesen:

3. Der Theiler eines Productes von zwei oder mehr ganzen Functionen Φ ist gleich dem Product der Theiler der einzelnen Factoren.

Die ganzen Functionen in Ω hängen ausser von den Variablen von einer algebraischen Zahl Θ ab, enthalten aber sonst nur rationale Zahlencoëfficienten. Bezeichnen wir eine solche Function mit $\varphi(\Theta, x, y, z, \ldots)$, so erhalten wir die conjugirten Functionen $\varphi, \varphi_1, \varphi_2, \ldots$ oder

(5) $\varphi(\Theta, x, y, z, \ldots),\quad \varphi(\Theta_1, x, y, z, \ldots),\quad \varphi(\Theta_2, x, y, z, \ldots), \ldots$

wenn wir für Θ die sämmtlichen Wurzeln der irreduciblen Gleichung $f(x) = 0$ [§. 132, (2)] einsetzen. Diese conjugirten Functionen können auch zum Theil einander gleich sein.

Sie sind alle einander gleich, wenn φ eine Function in R ist, und es ist umgekehrt φ eine Function in R, wenn die conjugirten Functionen alle einander gleich sind; denn es ist dann, wenn wir unter $S(\varphi)$ die Summe der conjugirten Functionen (die Spur) verstehen,

$$n \varphi = S(\varphi),$$

und $S(\varphi)$ ist eine ganze Function, deren Coëfficienten symmetrische Functionen der n Wurzeln Θ, d. h. rationale Zahlen, sind.

Zu den ganzen Functionen in R gehört auch die Norm von φ, d. h. das Product

(6) $N(\varphi) = \varphi\, \varphi_1\, \varphi_2 \ldots,$

denn alle Coëfficienten dieser Function sind symmetrische Functionen der Θ. Diese Function ist theilbar durch φ, und wenn wir

$$N(\varphi) = \varphi\, \varphi'$$

setzen, so sind sowohl φ als φ' ganze Functionen in Ω. Denn φ' ist als Product $\varphi_1\, \varphi_2 \ldots$ eine ganze Function, und die Coëffi-

cienten von φ' sind symmetrische Functionen der Wurzeln der Gleichung

$$\frac{f(x)}{x - \Theta} = 0,$$

die ihrerseits in Ω enthalten sind.

Aus der Definition ergiebt sich, dass die Norm eines Productes gleich dem Producte der Normen der Factoren ist, dass also, wenn φ, ψ Functionen in Ω sind,

(7) $$N(\varphi\psi) = N(\varphi)\, N(\psi)$$

ist.

§. 136.

Die Functionale eines algebraischen Körpers Ω und der erweiterte Körper $\overline{\Omega}$.

Die Variablen, die in der Theorie der algebraischen Zahlen verwendet werden, haben nicht die Bedeutung von Zeichen für veränderliche Zahlenreihen, wie man es aus der Functionentheorie gewöhnt ist, sondern sie sind lediglich Rechnungssymbole ohne eine selbständige Bedeutung. Bei den Functionen dieser Variablen kommt es eigentlich nur auf die Coëfficientensysteme an, und die Variablen werden nur dazu benutzt, um die bekannten und geläufigen Regeln der Buchstabenrechnung auf diese Coëfficientensysteme anzuwenden. Es ist damit freilich nicht ausgeschlossen, dass gelegentlich auch die Zahlen betrachtet werden, die man erhält, wenn man die Variablen durch gewisse Zahlen, z. B. durch rationale Zahlen, ersetzt.

Demnach führen wir in unsere Betrachtungen sowohl ganze als gebrochene Functionen von beliebig vielen Veränderlichen ein, deren Coëfficienten Zahlen eines algebraischen Körpers Ω sind, und setzen fest, dass mit diesen Functionen so gerechnet wird, wie es die Buchstabenrechnung vorschreibt.

Jede solche Function ω kann als Quotient zweier ganzer Functionen in Ω,

(1) $$\omega = \frac{\varphi}{\psi},$$

dargestellt werden, wobei ψ immer von Null verschieden angenommen werden muss. Zwei solche Functionen sind nur dann einander gleich:

$$\frac{\varphi}{\psi} = \frac{\varphi_1}{\psi_1},$$

wenn $\varphi \psi_1 = \varphi_1 \psi$ ist. Haben die beiden Functionen φ, ψ keinen gemeinsamen Theiler, so heisst $\varphi : \psi$ ein irreducibler Bruch. Unter den verschiedenen Darstellungen einer Function ω giebt es eine durch einen irreduciblen Bruch, und diese wollen wir die einfachste Darstellung nennen. In ihr sind Zähler und Nenner bis auf einen gemeinsamen Factor, der eine beliebige Zahl in Ω sein kann, durch ω selbst völlig bestimmt (Bd. I, §. 141).

Eine solche Function ω wollen wir ein Functional des Körpers Ω nennen. Als specielle Fälle sind darunter die ganzen Functionen und die Zahlen selbst enthalten. Bei den Zahlen ist jede Darstellung als Quotient zweier Zahlen in Ω als einfachste Darstellung zu betrachten.

Auf die Functionale lassen sich die vier Grundrechnungsarten in demselben Umfange anwenden, wie auf die Zahlen, und der Inbegriff aller Functionale des Körpers Ω ist daher gleichfalls ein Körper, den wir mit $\overline{\Omega}$ bezeichnen und den Functionalkörper von Ω nennen wollen[1].

Der Functionalkörper $\overline{\Omega}$ enthält den Zahlkörper Ω als Theiler.

Ein Functional, dessen Coëfficienten rationale Zahlen sind, heisst ein rationales Functional. Der Inbegriff aller rationalen Functionale ist der Functionalkörper $\overline{R}$ des Körpers R der rationalen Zahlen, und der Körper $\overline{R}$ ist in jedem algebraischen Functionalkörper $\overline{\Omega}$ enthalten.

Jedes rationale Functional A kann als Quotient zweier ganzer Functionen in R dargestellt werden, denen man auch ganzzahlige Coëfficienten geben kann, indem man Zähler und Nenner mit dem Hauptnenner aller Coëfficienten multiplicirt.

---

[1]) Es liegt nahe, die Functionale des Körpers Ω, mit denen wie mit den Zahlen in Ω gerechnet wird, geradezu als ideale Zahlen des Körpers Ω zu bezeichnen. Diese Ausdrucksweise würde sich einerseits an die Idealfactoren von Kummer, andererseits an die von Dedekind eingeführten Ideale anschliessen, die zu den Functionalen in einer sehr nahen, später zu erörternden Beziehung stehen. So bestechend in mancher Hinsicht eine solche Terminologie wäre, so erweist sie sich doch in anderer Hinsicht nicht als zweckmässig, weil dadurch den Functionalen, die doch immerhin nur Mittel zum Zweck, nicht selbständig für sich Gegenstand unseres Interesses sind, anscheinend eine grössere Bedeutung beigelegt würde, als ihnen in Wirklichkeit zukommt. Mit der Einführung des Wortes „Functional" folgen wir einem Vorschlage von Dedekind.

Sind in dieser Darstellung Zähler und Nenner imprimitiv, so kann man den Theiler herausnehmen und erhält eine Darstellung in der Form

$$(2) \qquad A = a\,\frac{E_1(x, y, z, \ldots)}{E_2(x, y, z, \ldots)} = a\,\frac{E_1}{E_2} = a\,E,$$

in der a eine positive, ganze oder gebrochene rationale Zahl ist, während E_1, E_2 primitive Functionen in R sind. Hieraus folgt:

1. **Man kann jedes rationale Functional durch Multiplication mit einer primitiven Function in R in eine ganze Function in R verwandeln, und mehrere rationale Functionale lassen sich als Brüche darstellen, deren gemeinsamer Nenner eine primitive Function ist.**

Die positive Zahl a und der Quotient $E_1 : E_2$ sind durch A vollständig bestimmt. Denn setzen wir a in die Form eines rationalen Bruches $q_1 : q_2$ und nehmen an, es sei

$$\frac{q_1}{q_2}\,\frac{E_1}{E_2} = \frac{q_1'}{q_2'}\,\frac{E_1'}{E_2'},$$

so folgt

$$q_1\,q_2'\,E_1\,E_2' = q_2\,q_1'\,E_2\,E_1'.$$

Hier haben wir also zwei ganze Functionen R mit ganzzahligen Coëfficienten, die einander gleich sind, und deren Theiler, da $E_1\,E_2'$ und $E_2\,E_1'$ primitive Functionen sind, $q_1\,q_2'$ oder $q_2\,q_1'$ ist. Folglich ist $q_1\,q_2' = q_2\,q_1'$, und daher auch

$$\frac{q_1}{q_2} = \frac{q_1'}{q_2'}, \quad \frac{E_1}{E_2} = \frac{E_1'}{E_2'}.$$

2. **Wir nennen die positive rationale Zahl a den absoluten Werth des Functionales A.**

In dem Falle, dass A selbst eine Zahl ist, ist a der absolute Werth von A in dem gewöhnlichen Sinne dieses Wortes, und E ist $= +1$ oder $= -1$ zu setzen, je nachdem A positiv oder negativ ist. Es ist also E nichts weiter als das Vorzeichen von A. In der weitgehenden Verallgemeinerung dieser elementaren Begriffe liegt das Befremdende, was unsere Definition dem ersten Blick bietet. Sie wird sich aber in der Folge als durchaus sachgemäss und nützlich erweisen.

Aus §. 135, 3. ergiebt sich der Satz:

3. **Der absolute Werth eines Productes zweier oder mehrerer rationaler Functionale ist gleich dem Producte der absoluten Werthe der Factoren.**

Ist ω ein Functional des Körpers Ω, so ist $N(\omega)$ ein rationales Functional, und die Norm eines Productes oder eines Quotienten zweier Functionale ist gleich dem Producte oder dem Quotienten der Normen der Bestandtheile.

4. **Wir nennen den absoluten Werth des rationalen Functionales $N(\omega)$ die absolute Norm $N_a(\omega)$ von ω und setzen**

(3) $$N(\omega) = N_a(\omega)\, E(\omega).$$

$N_a(\omega)$ ist immer eine positive rationale Zahl, und $E(\omega)$ ist der Quotient zweier primitiver ganzer Functionen. Aus 3. folgt, wenn α, β zwei Functionale in Ω sind, die Formel

(4) $$N_a(\alpha\beta) = N_a(\alpha)\, N_a(\beta),$$

oder der Satz:

5. **Die absolute Norm eines Productes von Functionalen in Ω ist gleich dem Producte der absoluten Normen der Factoren.**

Wenn wir alle Coëfficienten eines Functionales in Ω durch die entsprechenden Zahlen eines zu Ω conjugirten Körpers Ω_1 ersetzen, so erhalten wir ein conjugirtes Functional. Der gesammte Functionalkörper $\overline{\Omega}$ geht dadurch in einen conjugirten Functionalkörper $\overline{\Omega}_1$ über. Da jede Gleichung zwischen Functionalen des Körpers Ω im Grunde nur die Zusammenfassung einer Reihe von Gleichungen zwischen Zahlen des Körpers Ω ist, so haben wir den Satz (Bd. I, §. 141):

6. **Jede Gleichung zwischen Functionalen des Körpers $\overline{\Omega}$ bleibt richtig, wenn für alle Functionale die entsprechenden Elemente eines conjugirten Körpers $\overline{\Omega}_1$ gesetzt werden.**

Bedeutet t eine in ω nicht vorkommende Variable, so hat die Function $N(t - \omega)$ die Form

(5) $$\Phi(t) = t^n + A_1 t^{n-1} + A_2 t^{n-2} + \cdots + A_n,$$

worin die Coëfficienten A_i rationale Functionale sind, und diese Function $\Phi(t)$ verschwindet, wenn ω für t gesetzt wird. Es giebt aber nicht bloss eine solche Function $\Phi(t)$, die für $t = \omega$ ver-

schwindet, sondern beliebig viele, da man jedes $\Phi(t)$ mit einer beliebigen Function der gleichen Form multipliciren kann. Auch kann es vorkommen, dass schon ein Product von weniger als n Factoren von $N(t - \omega)$ rationale Coëfficienten erhält, woraus Functionen $\Phi(t)$ von niedrigerem als dem n^{ten} Grade entspringen, die für $t = \omega$ verschwinden. Daraus folgt:

7. Es giebt für jedes Functional ω des Körpers Ω unendlich viele Functionen $\Phi(t)$, die für $t = \omega$ verschwinden, in denen die höchste Potenz von t den Coëfficienten 1 hat, und deren übrige Coëfficienten in $\overline{R}$ enthalten sind.

Wir sagen dann, ω ist eine Wurzel der Gleichung

$$\Phi(t) = 0.$$

Unter den verschiedenen Functionen $\Phi(t)$, deren Existenz im Satze 7. ausgesprochen ist, giebt es eine und nur eine $F(t)$ von möglichst niedrigem Grade. Denn existiren zwei solche Functionen $F(t)$ und $F_1(t)$ von gleichem Grade m, so ist die Differenz $F(t) - F_1(t)$ in Bezug auf t höchstens vom Grade $m - 1$ und verschwindet für $t = \omega$. Dividirt man durch den Coëfficienten der höchsten Potenz von t, so erhält man eine Function $\Phi(t)$ von niedrigerem Grade als $F(t)$, die nach der Voraussetzung über $F(t)$ nicht existirt.

Die Function $F(t)$ kann im Körper $\overline{R}$ nicht in Factoren zerlegt werden, die ganze Functionen von t sind. Denn zerfiele sie in mehrere Factoren derselben Form $F_1(t)$, $F_2(t)$, so müsste einer dieser Factoren, die doch alle von niedrigerem Grade als $F(t)$ selbst sind, für $t = \omega$ verschwinden, entgegen unserer Voraussetzung.

Jede Function $\Phi(t)$ des Satzes 7. ist dann durch diese irreducible Function $F(t)$ theilbar, so dass der Quotient $\Phi(t) : F(t)$ eine ganze Function von t in $\overline{R}$ ist, in der die höchste Potenz von t den Coëfficienten 1 hat (vgl. Bd. I, §. 141, I.).

Unter den Functionen $\Phi(t)$ findet sich, wie schon bemerkt, auch die Norm $N(t - \omega)$, und folglich ist $N(t - \omega)$ durch $F(t)$ theilbar. Sind beide Functionen von gleichem Grade, so ist $N(t - \omega) = F(t)$. Ist aber der Grad von $F(t)$ niedriger als n, so verschwindet der Quotient $N(t - \omega) : F(t)$ wenigstens noch für eines der mit ω conjugirten Functionale, und folglich für alle; folglich auch für $t = \omega$, und daher ist dieser Quotient

nochmals durch $F(t)$, d. h. $N(t-\omega)$ ist durch $F(t)^2$ theilbar. Durch Fortsetzung dieses Schlussverfahrens erkennt man, dass $N(t-\omega)$ eine Potenz von $F(t)$ sein muss, und dass folglich der Grad von $F(t)$ ein Theiler von n ist (Bd. I, §. 144).

Wir fassen dies noch in dem Satz zusammen:

8. Jedes Functional in Ω ist die Wurzel einer und nur einer irreduciblen Gleichung $F(t) = 0$ in $\bar{R}$ und $N(t-\omega)$ ist eine Potenz von $F(t)$.

§. 137.

Ganze Functionale.

1. **Definition:** Ein rationales Functional soll ganz genannt werden, wenn sein absoluter Werth eine ganze Zahl ist.

Es ergiebt sich aus dieser Definition zunächst, dass die Summe, die Differenz und das Product von zwei und folglich auch von beliebig vielen ganzen rationalen Functionalen wieder ganz sind. Für das Product ist dies eine unmittelbare Folge des Satzes §. 136, 3. Um aber den Beweis für die Summe und die Differenz zu führen, stellen wir zwei ganze rationale Functionale A_1, A_2 so durch gebrochene Functionen dar, dass sie eine primitive Form als gemeinschaftlichen Nenner erhalten:

$$A_1 = a_1 \frac{E_1}{E}, \quad A_2 = a_2 \frac{E_2}{E}.$$

Dann ist

$$A_1 \pm A_2 = \frac{a_1 E_1 \pm a_2 E_2}{E},$$

da nun a_1, a_2 ganze Zahlen sind, so ist der Theiler der ganzen Function $a_1 E_1 \pm a_2 E_2$ der absolute Werth von $A_1 \pm A_2$. Dieser ist eine ganze Zahl, also $A_1 \pm A_2$ ein ganzes Functional.

Für constante rationale Functionale, d. h. für rationale Zahlen, giebt die Definition 1. die ganzen rationalen Zahlen.

Wir stellen ferner, ebenso wie im §. 133 für die Zahlen, folgende Definition der ganzen Functionale des Körpers Ω auf.

2. **Definition:** Ein Functional ω aus Ω heisst ganz, wenn es die Wurzel einer Gleichung

$$\Phi(t) = t^m + A_1 t^{m-1} + A_2 t^{m-2} + \cdots + A_m = 0$$

ist, in der die Coëfficienten $A_1, A_2, \ldots, A_m$ ganze rationale Functionale sind.

Functionale, die nicht zu den ganzen gehören, werden wir gelegentlich auch der Kürze wegen als gebrochene Functionale bezeichnen.

Zur Rechtfertigung dieser Definition beweisen wir zunächst den Satz:

3. Ist ω ein ganzes Functional nach der Definition 2. und zugleich rational, so ist es ein ganzes rationales Functional (nach der Definition 1.).

Angenommen, es sei ω ein gebrochenes rationales Functional, und daher der absolute Werth von ω ein rationaler Bruch $p : q$, worin p und q ganze rationale Zahlen ohne gemeinsamen Theiler sind; dann ist $q\,\omega$ ein ganzes rationales Functional, dessen absoluter Werth $= p$, also relativ prim zu q ist. Wenn aber andererseits ω zugleich ganz im Sinne der Definition 2. ist, so können wir

$$\omega^m = -(A_1\,\omega^{m-1} + A_2\,\omega^{m-2}\ldots)$$

setzen, woraus

$$(q\,\omega)^m = -\,q\,[A_1\,(q\,\omega)^{m-1} + A_2\,q\,(q\,\omega)^{m-2} + \cdots)$$

folgt.

Hieraus aber ergiebt sich, dass der absolute Werth p^m von $(q\,\omega)^m$ durch q theilbar sein muss, was nur möglich ist, wenn $q = 1$ ist. Die Definition 1. ist also in der Definition 2. als Specialfall enthalten.

Ist

$$\Phi(t) = t^m + A_1\,t^{m-1} + A_2\,t^{m-2} + \cdots + A_m$$

eine Function von t, in der die Coëfficienten $A_1, A_2, \ldots, A_m$ gebrochene rationale Functionale mit den Variablen $x, y, \ldots$, aber von der Variablen t frei sind, so kann man eine Function $a\,E(x, y, \ldots)$ bestimmen, in der a den Hauptnenner der absoluten Werthe von $A_1, A_2, \ldots$ und $E(x, y, \ldots)$ eine primitive ganze Function bedeutet, so dass

$$(1) \qquad a\,E\,(x\ y, \ldots)\,\Phi(t) = P\,(t, x, y, \ldots)$$

selbst eine primitive ganze Function ist [§. 136, 2.].

Zerfällt $\Phi(t)$ in zwei Factoren $\Phi_1(t)$, $\Phi_2(t)$ in R, ist also

$$\Phi\,(t) = \Phi_1\,(t)\,\Phi_2\,(t),$$

so bestimme man hiernach für die beiden Functionen Φ_1, Φ_2 die Factoren $a_1\,E_1$, $a_2\,E_2$, so dass

$$a_1 E_1 \Phi_1 = P_1, \quad a_2 E_2 \Phi_2 = P_2$$

primitive Functionen werden, und dann ist auch

(2) $$a_1 a_2 E_1 E_2 \Phi = P_1 P_2$$

eine primitive Function. Aus (1) und (2) folgt

(3) $$a_1 a_2 E_1 E_2 P = a E P_1 P_2$$

und mithin

(4) $$a = a_1 a_2.$$

Wenn also $a = 1$ ist, so müssen die natürlichen Zahlen a_1, a_2 auch $= 1$ sein, und wir haben den Satz:

4. Ist ω ein ganzes Functional in Ω und $\Phi(t)$ eine Function von t mit ganzen Coëfficienten in $\overline{R}$, die für $t = \omega$ verschwindet, so hat auch jeder rationale Theiler von $\Phi(t)$ ganze Coëfficienten in $\overline{R}$; insbesondere hat die irreducible Function $F(t)$, von der ω nach §. 136, 8. eine Wurzel ist, ganze rationale Functionale zu Coëfficienten.

Dieser Satz ist deshalb von principieller Bedeutung, weil er lehrt, dass ein Functional ω, das im Körper Ω zu den gebrochenen gehört, nicht etwa in einem höheren Körper als ganzes Functional erscheinen kann.

Wenn ein Functional ω nicht ganz ist, so genügt es einer Gleichung

$$\Phi(\omega) = \omega^m + A_1 \omega^{m-1} + A_2 \omega^{m-2} + \cdots + A_m = 0,$$

worin die Coëfficienten $A_1, A_2, \ldots, A_m$ zwar rationale, aber nicht ganze Functionale sind. Ist a der Hauptnenner der absoluten Werthe von $A_1, A_2, \ldots, A_m$, so sind $a A_1, a A_2, \ldots, a A_m$ ganze Functionale. Nun ist

$$a^m \Phi(\omega) = (a\omega)^m + a A_1 (a\omega)^{m-1} + a^2 A_2 (a\omega)^{m-2} + \cdots + a^m A_m = 0,$$

und $a\omega$ ist daher ein ganzes Functional. Daraus folgt:

5. Jedes Functional ω des Körpers Ω lässt sich durch Multiplication mit einer ganzen rationalen Zahl in ein ganzes Functional verwandeln, und daher kann man jedes Functional ω als Quotienten zweier ganzer Functionale darstellen. Diese Darstellung ist auf unendlich viele verschiedene Arten möglich, unter anderem so, dass der Nenner eine natürliche Zahl ist.

6. Ist ω ein Functional in Ω und giebt es m Grössen $\omega_1, \omega_2, \ldots, \omega_m$, die nicht alle verschwinden, von der Art, dass die m Producte $\omega\,\omega_i$ für $i = 1, 2, \ldots, m$ in die Form gesetzt werden können:

$$\omega\,\omega_i = A_{1,i}\,\omega_1 + A_{2,i}\,\omega_2 + \cdots + A_{m,i}\,\omega_m,$$

worin die m^2 Symbole $A_{k,i}$ ganze rationale Functionale sind, so ist ω ein ganzes Functional.

Hierin ist m irgend eine natürliche ganze Zahl. Die ω_i sind der Anwendung immer Zahlen oder Functionale in Ω, jedoch ; für die Gültigkeit des Satzes nur die Ausführbarkeit der in) angedeuteten Multiplication wesentlich.

Der Satz ist eine einfache Folge der Definition der ganzen ınctionale; denn da die ω_i nicht alle verschwinden, so muss ch dem Determinantensatze (Bd. I, §. 24, II.)

$$\begin{vmatrix} A_{1,1} - \omega, & A_{2,1}, & \ldots, & A_{m,1} \\ A_{1,2}, & A_{2,2} - \omega, & \ldots, & A_{m,2} \\ \cdot & \cdot & \cdot & \cdot \\ A_{1,m}, & A_{2,m}, & \ldots, & A_{m,m} - \omega \end{vmatrix} = 0$$

.n. Durch Ordnen nach Potenzen von ω ergiebt sich hieraus ıe Gleichung

$$\omega^m + A_1\,\omega^{m-1} + \cdots + A_m = 0,$$

ırin die Coëfficienten $A_1, A_2, \ldots$ durch Addition und Multication aus den $A_{i,k}$ zusammengesetzt sind und daher nach ganze rationale Functionale sind; demnach ist auch ω ein nzes Functional.

Für den letzten Coëfficienten A_m in der Gleichung (7) erlten wir den Ausdruck

$$(-1)^m A_m = \Sigma \pm A_{1,1}\,A_{2,2} \ldots A_{m,m},$$

r also gleich dem Producte der sämmtlichen Wurzeln r Gleichung (7) ist.

Der Satz 4. ist wichtig als Kennzeichen für ganze Funcnale; er dient uns hier zum Beweise des folgenden Satzes:

7. Ist $\Psi(x, y, \ldots)$ eine ganze Function, deren Coëfficienten ganze rationale Zahlen oder Functionale, aber frei von den Variablen $x, y, \ldots$ sind, sind ferner $\alpha, \beta, \ldots$ ganze Functionale in Ω, so ist

$$\omega = \Psi(\alpha, \beta, \ldots)$$

auch ein ganzes Functional.

Es seien nämlich $\mu, \nu, \ldots$ die Grade der ganzzahligen Gleichungen, denen (nach 2.) die Functionale $\alpha, \beta, \ldots$ genügen, und $m = \mu \nu \ldots$ Wir verstehen unter $\omega_1, \omega_2, \ldots, \omega_m$ die m Grössen

$$\alpha^r \beta^s \ldots \quad r = 0, 1, \ldots, \mu - 1, \quad s = 0, 1, \ldots, \nu - 1, \ldots$$

Dann können mit Hülfe der Gleichungen $\mu^{ten}, \nu^{ten}, \ldots$ Grades, denen die Zahlen $\alpha, \beta, \ldots$ genügen, alle Producte $\alpha^r \beta^s \ldots$, in denen einer der Exponenten $r, s, \ldots$ grösser als $\mu - 1, \nu - 1, \ldots$ ist, linear in der Form (5) durch $\omega_1, \omega_2, \ldots, \omega_m$ ausgedrückt werden, und dasselbe gilt daher auch von jedem Functional ω und folglich auch von den Producten $\omega \omega_1, \omega \omega_2, \ldots, \omega \omega_m$. Daraus folgt nach 6., dass ω ganz ist, wie wir beweisen wollten.

Als speciellen Fall des Satzes 7., aus dem übrigens der allgemeine Satz leicht wieder gefolgert werden kann, heben wir hervor:

8. Durch Addition, Subtraction und Multiplication ganzer Functionale entstehen immer wieder ganze Functionale.

Wir haben schon früher (§. 134) bemerkt, dass man immer einen algebraischen Körper bestimmen kann, der beliebig gegebene algebraische Zahlen enthält. Daraus folgt, dass in dem Satze 7. die $\alpha, \beta, \ldots$ beliebige ganze algebraische Zahlen oder Functionale sein können, und Entsprechendes gilt von dem Satze 8.

Aus der Definition 2. folgt noch nach dem Satze §. 136, 8.:

9. Ist ω ein ganzes Functional des Körpers Ω, so sind auch alle mit ω conjugirte Functionale ganz.

Als besondere Folgerung dieses Satzes sei noch erwähnt:

10. Die absolute Norm eines ganzen Functionales ist eine natürliche ganze Zahl.

Wir beweisen endlich noch den folgenden Satz:

11. Wenn ein Functional ω einer Gleichung von der Form

$$\omega^m + \alpha_1 \omega^{m-1} + \cdots + \alpha_m = 0 \tag{10}$$

genügt, in der $\alpha_1, \alpha_2, \ldots, \alpha_m$ ganze Functionale in Ω sind, so ist auch ω ein ganzes Functional.

Um ihn zu beweisen, bezeichnen wir mit t eine in den α und in ω nicht vorkommende Variable und setzen

$$(11) \qquad \varphi(t) = t^m + \alpha_1 t^{m-1} + \cdots + \alpha_m.$$

Dann ist, wenn n der Grad des Körpers Ω ist,

$$\Phi(t) = N[\varphi(t)]$$

eine ganze Function mn^{ten} Grades von t, deren Coëfficienten ganze rationale Functionale sind. Zugleich ist $\Phi(\omega) = 0$, und folglich ω eine ganze Zahl.

Daraus folgt noch, dass der Satz 6. richtig bleibt, wenn die Coëfficienten $A_{k,i}$ nicht ganze Functionale in R, sondern in Ω sind.

Ist ein ganzes Functional ω zugleich eine Zahl, so ist es eine ganze Zahl, weil in diesem Falle $N(t - \omega)$ ganze rationale Zahlen zu Coëfficienten hat. Die ganzen Zahlen, die wir im §. 133 betrachtet haben, sind demnach als specielle Fälle unter den ganzen Functionalen enthalten.

§. 138.

Theilbarkeit. Associirte Functionale. Einheiten.

Die ganzen Functionale unterliegen ähnlichen Gesetzen der Theilbarkeit, wie die ganzen rationalen Zahlen. Um sie zu erkennen, stellen wir folgende Definition an die Spitze:

1. Ein ganzes Functional α heisst durch ein anderes, von Null verschiedenes ganzes Functional β theilbar, wenn der Quotient $\alpha : \beta = \gamma$ ein ganzes Functional ist.

Es ist dann $\alpha = \beta\gamma$ und β und γ heissen Theiler von α, und man sagt auch, β und γ gehen in α auf. Die Zahl 0 ist durch jedes ganze Functional theilbar.

Aus dieser Definition ergeben sich ohne Schwierigkeit die folgenden fundamentalen Sätze über Theilbarkeit:

2. Sind α und α_1 theilbar durch β, so ist auch $\alpha \pm \alpha_1$ theilbar durch β.

Denn ist $\alpha = \beta\gamma$, $\alpha_1 = \beta\gamma_1$, so ist $\alpha \pm \alpha_1 = \beta(\gamma \pm \gamma_1)$, und wenn γ und γ_1 ganz sind, so ist auch $\gamma \pm \gamma_1$ ganz.

3. **Ist α theilbar durch β, und β theilbar durch γ, so ist auch α theilbar durch γ.**

Denn nach der Voraussetzung giebt es zwei ganze Functionale $\varkappa$, λ, die den Bedingungen $\alpha = \varkappa\beta$, $\beta = \lambda\gamma$ genügen. Demnach ist auch $\alpha = \varkappa\lambda\gamma$, und da $\varkappa\lambda$ ganz ist, so ist α durch γ theilbar.

Ein Product $\beta\gamma$ zweier ganzer Functionale ist sowohl durch β als durch γ theilbar, und folglich ist, wenn β durch α theilbar ist, auch $\beta\gamma$ durch α theilbar. Aus diesen Sätzen ergiebt sich:

4. **Sind $\alpha, \beta, \ldots$ durch δ theilbar, und sind $\xi, \eta, \ldots$ beliebige ganze Functionale, so ist $\xi\alpha + \eta\beta + \ldots$ durch δ theilbar.**

Selbstverständlich erstrecken sich diese Definitionen und Sätze auch auf den Fall, dass Zahlen an die Stelle von Functionalen treten, und so erhalten wir die Theilbarkeit ganzer Zahlen.

5. Zwei ganze Functionale α, β, die gegenseitig durch einander theilbar sind, heissen associirt.

6. Ein mit der natürlichen Zahl 1 associirtes ganzes Functional ε, d. h. jeder Theiler der Zahl 1, heisst eine Einheit.

Je nachdem ε ein Functional oder eine Zahl ist, ist ε eine functionale oder eine numerische Einheit.

Im Körper R der rationalen Zahlen sind als functionale Einheiten die primitiven ganzen Functionen und die Quotienten von zweien unter ihnen anzusehen. Numerische Einheiten giebt es in R nur zwei, nämlich $+1$ und -1.

Ueber die hierdurch eingeführten Begriffe, die in enger gegenseitiger Beziehung stehen, leiten wir eine Reihe von Sätzen ab.

7. Sind α, β associirte Functionale, so sind die Quotienten $\beta : \alpha$ und $\alpha : \beta$ Einheiten.

Denn setzen wir $\beta = \alpha\varepsilon$, so ist ε ein ganzes Functional und $1 : \varepsilon = \alpha : \beta$ gleichfalls ganz; also ist ε ein Theiler der Zahl 1, d. h. ε ist eine Einheit.

8. Ist α ein ganzes Functional und ε eine Einheit, so sind α und $\alpha\varepsilon$ associirt.

Dies folgt unmittelbar aus der Definition; denn $\alpha : \alpha\varepsilon = 1 : \varepsilon$ und $\alpha\varepsilon : \alpha = \varepsilon$ sind beides ganze Functionale.

Eine Einheit ist ein ganzes Functional, dessen reciprokes gleichfalls ganz ist, und dieses reciproke Functional ist selbst eine Einheit. Durch eine Einheit ist jedes beliebige ganze Functional theilbar. Ueberhaupt gilt der Satz:

9. Das Product und der Quotient zweier Einheiten sind wieder Einheiten.

Denn sind ε_1, ε_2 zwei Einheiten, so sind $\varepsilon_1 \varepsilon_2$ und $1 : \varepsilon_1 \varepsilon_2$ ganze Functionale, also $\varepsilon_1 \varepsilon_2$ eine Einheit, und ebenso sind $\varepsilon_1 : \varepsilon_2$ und $\varepsilon_2 : \varepsilon_1$ ganz.

10. Ist ein ganzes Functional μ theilbar durch ein anderes, α, so ist jedes mit μ associirte Functional μ' auch durch jedes mit α associirte Functional α' theilbar.

Denn wenn $\mu : \alpha$ ganz und ε, ε_1 Einheiten sind, so ist auch $\mu \varepsilon : \alpha \varepsilon_1$ ganz.

11. Ist α associirt mit β und mit γ, so sind auch β und γ unter einander associirt.

Denn ist $\beta = \alpha \varepsilon$, $\gamma = \alpha \varepsilon_1$, so ist $\beta = \gamma \varepsilon : \varepsilon_1$, und $\varepsilon : \varepsilon_1$ ist nach 8. eine Einheit.

Ist α theilbar durch β, so ist die absolute Norm von α theilbar durch die absolute Norm von β, denn aus $\alpha = \beta \gamma$ folgt nach §. 136, 5.:

$$N_a(\alpha) = N_a(\beta)\, N_a(\gamma). \tag{1}$$

Daraus ergiebt sich weiter, dass die absolute Norm einer Einheit $= 1$ sein muss. Es gilt aber auch das Umgekehrte:

12. Ein ganzes Functional, dessen absolute Norm $= 1$ ist, ist eine Einheit.

Denn ist ε ein ganzes Functional mit der absoluten Norm 1, so ist $N(\varepsilon)$ ein ganzes rationales Functional mit dem absoluten Werthe 1, und daher ist auch $1 : N(\varepsilon)$ ein ganzes Functional. Setzen wir dann

$$N(\varepsilon) = \varepsilon \varepsilon',$$

so ist ε' als Product von ganzen Functionalen (den Conjugirten zu ε) selbst ganz, und folglich ist auch

$$\frac{1}{\varepsilon} = \frac{\varepsilon'}{N(\varepsilon)}$$

ein ganzes Functional, also ε eine Einheit.

Daraus schliessen wir noch nach der Formel (1), dass associirte Functionale dieselbe absolute Norm haben.

Ein ganzes rationales Functional ist hiernach immer mit seinem absoluten Werthe associirt. Ist also α irgend ein ganzes Functional des Körpers $\overline{\Omega}$, so sind auch $N(\alpha)$ und $N_a(\alpha)$ associirt. Da nun in $N(\alpha) = \alpha\alpha'$ der Factor α' als Product von ganzen Functionalen selbst ganz ist, so ist $N(\alpha)$ und folglich auch die natürliche Zahl $N_a(\alpha)$ durch α theilbar. Wir formuliren also noch den Satz:

13. Es giebt natürliche ganze Zahlen (in unendlicher Menge), darunter die absolute Norm von α, die durch ein beliebiges ganzes Functional α theilbar sind. Ist a die kleinste unter den durch α theilbaren natürlichen Zahlen, so ist jede durch α theilbare ganze rationale Zahl durch a theilbar.

Denn ist m eine durch α theilbare ganze rationale Zahl, so ist auch der Rest der Division von m durch a eine durch α theilbare, ganze rationale Zahl. Da diese kleiner als a ist, so muss sie $= 0$ sein.

§. 139.

Grösster gemeinschaftlicher Theiler.

Es mögen $\alpha, \beta, \ldots$ von Null verschiedene ganze Functionale in Ω in beliebiger aber endlicher Anzahl bedeuten, und $x, y, \ldots$ Variable, die in $\alpha, \beta, \ldots$ nicht vorkommen. Dann ist

$$(1) \qquad \delta = \alpha x + \beta y + \cdots$$

gleichfalls ein ganzes Functional in Ω. Die Norm von δ ist eine ganze homogene Function n^{ten} Grades der Variablen $x, y, \ldots$ deren Coëfficienten ganze rationale Functionale sind. Bezeichnen wir die absolute Norm von δ mit D, so ist

$$(2) \qquad N(\delta) = D E(x, y, \ldots) = D E,$$

und darin ist $E(x, y, \ldots) = E$ eine ganze rationale Function der Variablen $x, y, \ldots$ und im Allgemeinen eine gebrochene Function der in $\alpha, \beta, \ldots$ vorkommenden Variablen, jedenfalls aber eine rationale Einheit [§. 136, (2)].

Wir wollen jetzt unter $x_0, y_0, \ldots$ irgend welche ganze rationale Zahlen verstehen. Dann ist auch

$$\delta_0 = \alpha x_0 + \beta y_0 + \cdots$$

ein ganzes Functional, und wir wollen beweisen, dass δ_0 durch δ theilbar ist.

Wir brauchen zu diesem Zwecke nur das ganze Functional

$$\delta t - \delta_0 = \alpha (x t - x_0) + \beta (y t - y_0) \ldots$$

zu betrachten, worin t eine neue Variable bedeutet. Dann ist [nach (2)]:

(3) $$N(\delta t - \delta_0) = D E (x t - x_0, y t - y_0, \ldots),$$

oder, indem wir nach absteigenden Potenzen von t ordnen:

(4) $$N(\delta t - \delta_0) = D (t^n E + t^{n-1} E_1 + t^{n-2} E_2 + \cdots),$$

worin $E_1, E_2, \ldots$ nach §. 137, 7., 8. ganze rationale Functionale sind. Setzen wir nun

$$C_1 = \frac{E_1}{E}, \quad C_2 = \frac{E_2}{E}, \cdots,$$

so sind, da E eine Einheit ist, auch $C_1, C_2, \ldots$ ganze rationale Functionale, und es folgt, wenn wir noch

$$\frac{\delta_0}{\delta} = \eta$$

setzen, aus (4)

$$N(\delta) N(t - \eta) = D E (t^n + C_1 t^{n-1} + C_2 t^{n-2} + \cdots),$$

oder wegen (2)

(5) $$N(t - \eta) = t^n + C_1 t^{n-1} + C_2 t^{n-2} + \cdots$$

Da diese Function nun verschwindet, wenn $t = \eta$ gesetzt wird, so folgt, dass η ein ganzes Functional ist (§. 137, 2.), und damit ist bewiesen, dass δ_0 durch δ theilbar ist.

Da $x_0, y_0, \ldots$ beliebige ganze rationale Zahlen bedeuten können, so schliessen wir daraus, dass die Functionale $\alpha, \beta, \ldots$ selbst durch δ theilbar sind, dass also δ ein gemeinsamer Theiler der Functionale $\alpha, \beta, \ldots$ ist.

Andererseits ist aber auch (nach §. 138, 4.) δ durch jeden gemeinsamen Theiler von $\alpha, \beta, \ldots$ theilbar, und δ hat also die charakteristischen Eigenschaften des grössten gemeinschaftlichen Theilers von $\alpha, \beta, \ldots$ Dieselben Eigenschaften kommen aber nach §. 138, 7. jedem mit δ associirten Functional zu, und ebenso sind auch zwei Functionale δ, δ', die diese doppelte Eigen-

schaft haben, durch einander theilbar, also associirt, und wir stellen also die Definition auf:

1. Das Functional $\delta = \alpha x + \beta y + \cdots$ und jedes damit associirte Functional heisst grösster gemeinschaftlicher Theiler von $\alpha, \beta, \ldots$

Wenn δ eine Einheit ist, so sagen wir auch, $\alpha, \beta, \ldots$ seien ohne gemeinsamen Theiler, denn dann giebt es ausser den Einheiten kein ganzes Functional, das in allen $\alpha, \beta, \ldots$ aufgeht.

2. Zwei Functionale α, β, die keinen gemeinsamen Theiler haben, für die also $\alpha x + \beta y$ eine Einheit ist, heissen relative Primfunctionale oder theilerfremd.

Aus diesen Definitionen ergeben sich sehr einfach folgende Sätze:

3. Wenn ganze Functionale $\xi, \eta, \ldots$ in Ω existiren, derart, dass
$$\alpha \xi + \beta \eta + \cdots = \varepsilon$$
eine Einheit ist, so sind die ganzen Functionale $\alpha, \beta, \ldots$ ohne gemeinsamen Theiler.

Denn haben $\alpha, \beta, \ldots$ einen gemeinsamen Theiler δ, so ist (nach §. 138) δ auch Theiler von $\alpha \xi + \beta \eta + \cdots$, und δ muss also auch eine Einheit sein.

4. Sind α, β, γ drei ganze Functionale und ist α relativ prim zu β und zu γ, so ist α auch relativ prim zu $\beta \gamma$.

Denn nach Voraussetzung sind, wenn x, y, u, v vier Variable sind,
$$\varepsilon = \alpha x + \beta y, \quad \varepsilon_1 = \alpha u + \gamma v$$
Einheiten. Demnach ist auch
$$\alpha (\alpha u x + \gamma v x + \beta u y) + \beta \gamma v y = \varepsilon \varepsilon_1$$
eine Einheit. Da aber $\alpha u x + \gamma v x + \beta u y$ und $v y$ ganz sind, so folgt nach dem Satze 3., dass α und $\beta \gamma$ relativ prim sind.

Hieran schliesst sich der Beweis des folgenden sehr wichtigen Satzes:

5. Sind α, β, μ ganze Functionale, α relativ prim zu β und $\alpha \mu$ durch β theilbar, so ist μ durch β theilbar.

Denn nach der Voraussetzung über α, β ist

$$\alpha x + \beta y = \varepsilon$$

eine Einheit. Durch Multiplication mit μ folgt daraus

$$\alpha \mu x + \beta \mu y = \varepsilon \mu,$$

und da $\alpha \mu$ und $\beta \mu$ nach Voraussetzung durch β theilbar sind, so ist auch $\varepsilon \mu$ und folglich auch das mit $\varepsilon \mu$ associirte μ durch β theilbar.

§. 140.

Primfunctionale im Körper Ω.

Durch die Sätze des vorigen Paragraphen haben wir die Hülfsmittel gewonnen, um die Gesetze der Theilbarkeit der ganzen Functionale im Körper Ω genau auf demselben Wege abzuleiten, den man in den Elementen der Arithmetik auf die natürlichen ganzen Zahlen anwendet. Wir definiren folgendermaassen:

1. Ein ganzes Functional π des Körpers Ω, welches keine Einheit ist, heisst ein Primfunctional, wenn es ausser durch die Einheiten nur noch durch die mit ihm selbst associirten Functionale theilbar ist. Jedes ganze Functional in Ω, das ausser diesen noch andere Theiler hat, heisst zusammengesetzt.

Der Begriff des Primfunctionales ist hiernach wesentlich von dem Körper Ω abhängig. Es können sehr wohl die Primfunctionale eines Körpers in einem anderen erweiterten Körper zusammengesetzt sein.

Wenn ω ein beliebiges ganzes und π ein Primfunctional des Körpers Ω ist, so sind nur zwei Fälle möglich: entweder ω ist relativ prim zu π oder ω ist durch π theilbar; denn ein gemeinschaftlicher Theiler von ω und π kann nur entweder eine Einheit oder mit π associirt sein, und im letzteren Falle ist ω durch π theilbar. Daraus ergiebt sich der Satz:

2. Wenn das Product $\alpha\beta$ zweier ganzer Functionale α, β in Ω durch ein Primfunctional π theilbar ist, so muss einer der beiden Factoren durch π theilbar sein.

Denn wenn α und β beide nicht durch π theilbar, also beide relativ prim zu π sind, so ist nach §. 139, 4. auch $\alpha\beta$ relativ prim zu π.

Es ergiebt sich daraus durch wiederholte Anwendung, dass, wenn ein Product aus mehreren Factoren durch π theilbar ist, mindestens einer der Factoren durch π theilbar sein muss.

3. Die kleinste natürliche ganze Zahl p, die durch ein Primfunctional π in Ω theilbar ist, ist eine natürliche Primzahl, und die absolute Norm von π ist eine Potenz von p. Jede durch π theilbare ganze rationale Zahl ist auch durch p theilbar.

Nach §. 138, 13. giebt es natürliche Zahlen, die durch π theilbar sind. Die kleinste unter ihnen, p, kann nicht in zwei natürliche Factoren, die grösser als 1 sind, zerlegbar sein; denn ist $p = p_1 p_2$, so muss entweder p_1 oder p_2 durch π theilbar sein (nach 2.). Ist aber keiner der Factoren $p_1, p_2 = 1$, so sind sie beide kleiner als p, was der Voraussetzung über p widerspricht. Folglich ist p eine natürliche Primzahl. Dass jede durch π theilbare natürliche Zahl m durch p theilbar ist, haben wir schon im §. 138, 13. bewiesen.

Setzen wir nun

$$p = \pi\,\omega, \tag{1}$$

so ist ω ein ganzes Functional, und wenn wir beiderseits die absoluten Normen nehmen, so folgt, da die absolute Norm einer natürlichen Zahl die n^{te} Potenz dieser Zahl ist:

$$p^n = N_a(\pi)\, N_a(\omega). \tag{2}$$

Hieraus folgt der zweite Theil unseres Satzes, dass die natürliche ganze Zahl $N_a(\pi)$ eine Potenz von p ist.

Setzen wir demnach

$$N_a(\pi) = p^f, \tag{3}$$

so ist f eine Zahl, die nur einen der Werthe $1, 2, 3, \ldots, n$ haben kann, wenn n den Grad des Körpers Ω bedeutet.

Die Zahl f heisst der Grad des Primfunctionals π.

§. 141.

Zerlegung der ganzen und gebrochenen Functionale in Primfactoren.

1. Jedes von Null verschiedene ganze Functional ω des Körpers Ω, das keine Einheit ist, ist durch ein Primfunctional theilbar.

Wenn ω prim ist, so ist der Satz evident, weil ω durch sich selbst theilbar ist. Wenn aber ω nicht prim ist, so ist es durch ein ganzes Functional ω_1 theilbar, das weder eine Einheit, noch mit ω associirt ist. Ist also

(1) $$\omega = \omega_1 \alpha,$$

so ist weder ω_1 noch α eine Einheit. Aus (1) folgt aber

$$N_a(\omega) = N_a(\omega_1)\, N_a(\beta),$$

und da $N_a(\beta)$ grösser als 1 ist, so ist

(2) $$N_a(\omega_1) < N_a(\omega).$$

Wenn ω_1 noch nicht prim ist, so kann man denselben Schluss auf ω_1 anwenden und findet einen Theiler ω_2 von ω_1 derart, dass

(3) $$N_a(\omega_2) < N_a(\omega_1) < N_a(\omega)$$

ist. Da es aber nur eine endliche Anzahl natürlicher Zahlen giebt, die kleiner sind als $N_a(\omega)$, so muss die Reihe der Functionale $\omega, \omega_1, \omega_2, \ldots$ abbrechen, und dies ist nur möglich, wenn das letzte von ihnen ein Primfunctional ist, wodurch der Satz 1. bewiesen ist.

2. Jedes ganze von Null und von den Einheiten verschiedene Functional ω im Körper Ω kann in eine endliche Anzahl von Primfactoren zerlegt werden.

Ist nämlich π_1 ein Primfactor von ω und

(4) $$\omega = \pi_1 \omega_1,$$

so ist, da $N_a(\pi_1) > 1$ ist,

$$N_a(\omega) > N_a(\omega_1).$$

Ist ω_1 keine Einheit, so ist es durch ein Primfunctional π_2 theilbar, und aus

$$\omega_1 = \pi_2 \omega_2$$

folgt

$$N_a(\omega_1) > N_a(\omega_2).$$

Fährt man so fort, so erhält man eine Reihe ganzer Functionale $\omega_1, \omega_2, \ldots$, deren absolute Normen fortwährend abnehmen, und diese Reihe bricht also mit einer Einheit ab. Ist π_ν die letzte von ihnen, die keine Einheit ist, so ist π_ν selbst ein Primfunctional, und es folgt

(5) $$\omega = \pi_1 \pi_2 \ldots \pi_\nu,$$

w. z. b. w.

3. **Ein ganzes Functional ω im Körper Ω ist nur auf eine Weise in Primfactoren zerlegbar, wenn associirte Primfactoren als nicht verschieden betrachtet werden. Associirte Functionale enthalten dieselben Primfactoren.**

Nehmen wir nämlich an, es seien die beiden Producte von Primfactoren

(6) $$\pi_1\,\pi_2\,\ldots\,\pi_\nu, \qquad \varkappa_1\,\varkappa_2\,\ldots\,\varkappa_\mu$$

mit einander associirt, so ist das Product $\pi_1\pi_2\ldots\pi_\nu$ durch den Primfactor $\varkappa_1$ theilbar, und es muss daher, nach §. 140, 2., einer der Factoren, etwa π_1, durch $\varkappa_1$ theilbar und folglich mit $\varkappa_1$ associirt sein. Dann sind auch die Producte

$$\pi_2\,\ldots\,\pi_\nu, \qquad \varkappa_2\,\ldots\,\varkappa_\mu$$

associirt, und folglich ist einer der Factoren des ersten Productes, etwa π_2, durch $\varkappa_2$ theilbar und daher mit $\varkappa_2$ associirt. So kann man weiter schliessen, und es ergiebt sich, dass nicht nur die Anzahl der $\varkappa$ mit der Anzahl der π übereinstimmen muss, sondern dass auch die $\varkappa$ einzeln den π associirt sind.

Unter den Primfactoren eines ganzen Functionales ω kann derselbe mehrmals vorkommen, und diese einander gleichen (oder associirten) Factoren können zu einer Potenz zusammengefasst werden. Ist ω durch π^h theilbar, so sagen wir, das Primfunctional π geht $h$mal in ω auf.

Hiernach hat es einen ganz bestimmten Sinn, wenn von den Primfactoren eines ganzen Functionales gesprochen wird. Wir folgern noch aus dem Bewiesenen:

4. **Ein ganzes Functional α ist dann und nur dann durch ein anderes β theilbar, wenn alle Primfactoren von β unter den Primfactoren von α vorkommen, und jeder von ihnen mindestens so oft in α aufgeht, als in β.**

Denn ist α durch β und β durch π^h theilbar, so ist auch α durch π^h theilbar.

Sind $\alpha, \beta, \ldots$ ganze Functionale, $\pi_1, \pi_2, \ldots$ verschiedene Primfunctionale, $\varepsilon_1, \varepsilon_2, \ldots$ Einheiten, so können wir Exponenten $a_1, a_2, \ldots, b_1, b_2, \ldots$ so bestimmen, dass

(7) $$\begin{aligned} \varepsilon_1\,\alpha &= \pi_1^{a_1}\,\pi_2^{a_2}\,\ldots \\ \varepsilon_2\,\beta &= \pi_1^{b_1}\,\pi_2^{b_2}\,\ldots \\ &\ldots\ldots\ldots \end{aligned}$$

wird, falls wir den Exponenten gleich Null setzen, wenn einer der Primfactoren in dem betreffenden Functionale nicht aufgeht. Ein gemeinsamer Theiler der Zahlen $\alpha, \beta, \ldots$ kann keine anderen Primfactoren als $\pi_1, \pi_2, \ldots$ enthalten, und jeder gemeinsame Theiler von $\alpha, \beta, \ldots$ hat die Form

(8) $$\varepsilon\, \delta = \pi_1^a\, \pi_2^b \ldots,$$

worin a nicht grösser als die kleinste der Zahlen $a_1, b_1, \ldots$ sein darf, b nicht grösser als die kleinste der Zahlen $a_2, b_2, \ldots$ u. s. f.

Ist a die kleinste unter den Zahlen $a_1, b_1, \ldots$, b die kleinste unter den Zahlen $a_2, b_2, \ldots$, so ist die in (8) dargestellte Zahl δ der grösste gemeinschaftliche Theiler der Zahlen $\alpha, \beta, \ldots$ In Worten ausgedrückt:

Man erhält den grössten gemeinschaftlichen Theiler mehrerer ganzer Functionale $\alpha, \beta, \ldots$, wenn man ein Product aus Primfactoren bildet, in das man jeden Primfactor so oft aufnimmt, als er in jeder der Zahlen $\alpha, \beta, \ldots$ aufgeht.

Zwei Zahlen sind relativ prim, wenn sie keinen gemeinschaftlichen Primfactor enthalten.

Dem entsprechend definiren wir als das kleinste gemeinschaftliche Multiplum μ der Functionale $\alpha, \beta, \ldots$ ein Product aus Primfactoren, in das wir einen Factor π so oft aufnehmen, dass er in keinem der Functionale $\alpha, \beta, \ldots$ öfter als in μ aufgeht. Dieses Functional μ hat dann, ebenso wie jedes mit μ associirte Functional, die doppelte, und, wie wir hinzufügen können, charakteristische Eigenschaft, dass es durch jedes der Functionale $\alpha, \beta, \ldots$ theilbar ist, und dass jedes andere Functional, das durch $\alpha, \beta, \ldots$ theilbar ist, auch durch μ theilbar ist.

Das kleinste gemeinschaftliche Multiplum zweier relativer Primfunctionale ist ihr Product.

Man kann diese Sätze anwenden, um gebrochene Functionale in der einfachsten Gestalt oder als reducirte Brüche darzustellen, indem man Zähler und Nenner in ihre Primfactoren zerlegt und den grössten gemeinschaftlichen Theiler weghebt. Zähler und Nenner eines reducirten Bruches sind durch den Bruch selbst völlig bestimmt, abgesehen von einem gemeinschaftlichen Einheitsfactor, der unbestimmt bleibt.

Ebenso kann man eine beliebige Zahl gegebener Brüche auf gemeinsamen Nenner, den Hauptnenner, bringen, indem man ein gemeinsames Multiplum aller gegebenen Nenner als gemeinschaftlichen Nenner wählt.

Sind die gegebenen Functionale wirkliche Brüche, d. h. reduciren sie sich nicht alle auf ganze Functionale, so muss der gemeinsame Nenner wenigstens einen Primfactor enthalten, der nicht in allen Zählern vorkommt.

Alles das ist in vollkommener Uebereinstimmung mit den Regeln der elementaren Arithmetik, und auch die Beweismethoden, die wir hier angewandt haben, sind wesentlich dieselben, die dort gebraucht werden. Der Kernpunkt der Deduction ist einerseits die weitgehende Verallgemeinerung des Begriffes der Einheit, andererseits die darauf gegründete Definition des grössten gemeinschaftlichen Theilers im §. 139.

§. 142.

Ganze Functionen im Körper $\overline{\mathfrak{Q}}$.

Die Hülfsmittel, über die wir jetzt verfügen, reichen aus, um die Schlussweise, deren wir uns im §. 2 des ersten Bandes zum Beweis des Gauss'schen Satzes bedient haben, auf die Functionale anzuwenden.

In der That ist ja der Satz, auf den sich jener Beweis wesentlich stützt, dass ein Product zweier ganzer Zahlen nur dann durch eine Primzahl theilbar ist, wenn diese Primzahl in einem der Factoren aufgeht, auch für die jetzt eingeführten Primfunctionale als gültig erwiesen.

Wir können demnach, indem wir dem erwähnten Beweise Schritt für Schritt folgen, den Satz als erwiesen ansehen:

1. Wenn zwei ganze Functionen einer Variablen t der Grade h und k:
$$\varphi = \alpha_0 t^h + \alpha_1 t^{h-1} + \cdots + \alpha_h$$
$$\psi = \beta_0 t^k + \beta_1 t^{k-1} + \cdots + \beta_k,$$
deren Coëfficienten ganze Functionale sind, die die Variable t nicht enthalten, ein Product
$$\chi = \gamma_0 t^{h+k} + \gamma_1 t^{h+k-1} + \cdots + \gamma_{h+k}$$
haben, in dem die Coëfficienten $\gamma_0, \gamma_1, \ldots, \gamma_{h+k}$ einen gemeinschaftlichen Primtheiler π haben, so muss π entweder in allen Coëfficienten von φ oder in allen Coëfficienten von ψ aufgehen.

Aus diesem Satze ziehen wir hier eine wichtige Folgerung: Die Functionen

(1) $$\varphi = \varphi_0 t^h + \varphi_1 t^{h-1} + \cdots + \varphi_h,$$

in denen die Coëfficienten $\varphi_0, \varphi_1, \ldots, \varphi_h$ ganze oder gebrochene Functionale in Ω sind, aber von den Variablen t frei angenommen werden, gehören selbst zu den Functionalen im Körper Ω. Von ihnen gilt der Satz:

2. Ein Functional φ ist nur dann ganz, wenn die Coëfficienten $\varphi_0, \varphi_1, \ldots, \varphi_h$ ganze Functionale sind.

Um ihn zu beweisen, nehmen wir an, es seien $\varphi_0, \varphi_1, \ldots, \varphi_h$ nicht alle zugleich ganz. Bestimmen wir ihren Hauptnenner μ und setzen

$$\mu\,\varphi_0 = \alpha_0,\ \mu\,\varphi_1 = \alpha_1,\ \ldots,\ \mu\,\varphi_h = \alpha_h,$$

so sind $\alpha_0, \alpha_1, \ldots, \alpha_h$ ganze Functionale, und μ enthält wenigstens einen Primfactor π, der nicht zugleich in allen Zählern $\alpha_0,, \alpha_1, \ldots, \alpha_h$ aufgeht (vgl. den Schluss des vor. Paragraphen).

Dann ist die Function

(2) $$\chi = \mu\,\varphi = \alpha_0 t^h + \alpha_1 t^{h-1} + \cdots + \alpha_h,$$

deren Coëfficienten nun ganz sind, gewiss ein ganzes Functional.

Nehmen wir nun an, es sei φ selbst ganz, so ist $\mu\,\varphi$ durch π theilbar, während doch nicht sämmtliche Coëfficienten $\alpha_0, \alpha_1, \ldots, \alpha_h$ durch π theilbar sind. Wenn nun φ ein ganzes Functional ist, so genügt es einer Gleichung von der Form

(3) $$\varphi^m = C_1\,\varphi^{m-1} + C_2\,\varphi^{m-2} + \cdots + C_m,$$

in der die Coëfficienten $C_1, C_2, \ldots, C_m$ ganze rationale Functionale sind.

Diese Functionale setzen wir nach §. 136, (2) in die Form

$$C_1 = \frac{a_1 E_1}{E},\ C_2 = \frac{a_2 E_2}{E},\ \ldots,\ C_m = \frac{a_m E_m}{E},$$

worin $a_1, a_2, \ldots, a_m$ die absoluten Werthe von $C_1, C_2, \ldots, C_m$, also natürliche ganze Zahlen (oder Null), und $E, E_1, \ldots, E_m$ primitive ganze Functionen, also Einheiten, sind.

Dann ergiebt die Gleichung (3):

$$E\,\varphi^m = a_1 E_1\,\varphi^{m-1} + a_2 E_2\,\varphi^{m-2} + \cdots + a_m E_m,$$

und durch Multiplication mit μ^m:

(4) $$E\,\chi^m = \mu(a_1 E_1\,\chi^{m-1} + a_2 E_2\,\mu\,\chi^{m-2} + \cdots + a_m E_m\,\mu^{m-1}).$$

Hier stehen nun rechter und linker Hand ganze Functionen von t, deren Coëfficienten ganze Functionale sind. Auf der rechten Seite haben alle diese Coëfficienten den Factor μ, also auch den Factor π, während nach Voraussetzung nicht alle Coëfficienten von χ diesen Factor haben. Da E eine Einheit ist, so enthalten auch die Coëfficienten von E den Factor π nicht, und folglich können nach dem Satze 1. auch die Coëfficienten von $E\chi^m$ nicht alle durch π theilbar sein, was doch die Gleichung (4) verlangen würde. Daraus ergiebt sich, dass unsere Annahme, φ sei ganz, $\varphi_0, \varphi_1, \ldots, \varphi_k$ dagegen nicht alle ganz, unstatthaft ist, und der Satz 2. ist somit bewiesen.

Nehmen wir nun an, in φ seien die Coëfficienten $\varphi_0, \varphi_1, \ldots$ selbst wieder ganze Functionen einer Variablen, und wenden den Satz 2. wiederholt darauf an, so gelangen wir zu dem Schlusse:

3. Eine ganze rationale Function beliebig vieler Veränderlicher, deren Coëfficienten Zahlen oder Functionale mit anderen Variablen sind, ist nur dann ein ganzes Functional, wenn die Coëfficienten ganz sind.

Wir können jedes Functional ω als Quotienten zweier ganzer Functionen in der Weise darstellen, dass der Nenner eine primitive Function im Körper R wird.

Denn sind φ, ψ ganze Functionen in Ω, und ist

$$\omega = \frac{\varphi}{\psi}, \quad N(\psi) = \psi\,\psi',$$

so können wir den Bruch ω durch ψ' erweitern und erhalten im Nenner eine ganze Function mit rationalen Coëfficienten. Den Theiler dieser Function können wir dann zum Zähler von ω rechnen, und erhalten, wenn E eine primitive Function, χ eine ganze Function in Ω bedeutet:

$$E\,\omega = \chi,$$

d. h. man kann jedes Functional ω in Ω durch Multiplication mit einer primitiven Function E in eine ganze Function der Variablen verwandeln, deren Coëfficienten Zahlen in Ω sind.

Mit Zuziehung des Satzes 3. ergiebt sich hieraus:

4. Jedes ganze Functional ω im Körper Ω ist associirt mit einer ganzen Function χ, deren Coëffi-

cienten ganze Zahlen in Ω sind, und geht durch Multiplication mit einem rationalen Functional, welches eine Einheit ist, in χ über.

§. 143.

Die Primfactoren der Zahlen des Körpers Ω.

Da unter den Functionalen des Körpers Ω auch die Zahlen enthalten sind, so ergiebt sich aus den Resultaten des §. 141, dass sich auch die ganzen Zahlen des Körpers Ω in Primfactoren zerlegen lassen, aber in Primfactoren, die im Allgemeinen nicht Zahlen, sondern Functionale sind. Es ist aber nicht ausgeschlossen, dass in besonderen Fällen unter den Primfunctionalen auch Zahlen auftreten können, die dann **Primzahlen** des Körpers Ω heissen.

Alle Gleichungen zwischen Functionalen sind in letzter Instanz identische Gleichungen zwischen ganzen rationalen Functionen und lösen sich in eine Reihe von Gleichungen zwischen Zahlen auf. Sie bleiben also richtig, wenn für die Variablen andere Zeichen gesetzt werden.

Es folgt daraus, dass ein ganzes Functional, eine Einheit, ein Primfunctional nicht aufhören, ganze Functionale, Einheiten, Primfunctionale zu sein, wenn für die Variablen andere Symbole gesetzt werden.

Zerlegen wir also eine Zahl in ihre Primfactoren, so können, wenn unter diesen Primfactoren Functionale vorkommen, in der diese Zerlegung darstellenden Gleichung die Variablen durch beliebige andere Variable ersetzt werden, und daraus folgt die Verallgemeinerung:

1. Man kann die Primfactoren eines ganzen Functionals ω so darstellen, dass sie die Variablen, von denen ω abhängt, nicht enthalten.

Denn jedes ganze Functional ω ist Theiler von Zahlen, sogar von rationalen Zahlen, z. B. von der absoluten Norm von ω. Die Primfactoren von ω sind daher unter den Primfactoren einer dieser Zahlen zu suchen und können also durch Variable dargestellt werden, die von den in ω vorkommenden verschieden sind.

Nach §. 142, 4. können wir, wenn ω ein gegebenes ganzes Functional, E eine Einheit, φ eine ganze Function in Ω ist, setzen:

$$(1) \qquad E\,\omega = \varphi\,(x, y, \ldots).$$

Wenn wir andererseits ω in seine Primfactoren zerlegen, so können wir nach 1. diese Primfactoren von den Variablen $x, y, \ldots$ frei annehmen, und wenn wir wieder das Product dieser Primfactoren bilden, so erhalten wir eine mit ω associirte Zahl ω_1, die von den Variablen $x, y, \ldots$ frei ist.

Ordnen wir den Quotienten $\varphi : \omega_1$, der eine ganze Zahl (sogar eine Einheit) ist, nach den Variablen $x, y, \ldots$, so schliessen wir aus §. 142, 3., dass alle Coëfficienten der Function φ durch ω_1 und folglich auch durch ω und φ theilbar sind.

Wenn andererseits alle Coëfficienten von φ durch irgend einen Factor δ in Ω theilbar sind, so ist auch φ durch δ theilbar, und daraus ergiebt sich:

2. Eine ganze Function φ mit ganzen Zahlen als Coëfficienten ist der grösste gemeinschaftliche Theiler aller ihrer Coëfficienten.

Die ganze Zahl φ geht also nach §. 139 in eine associirte Zahl über, wenn die einzelnen Potenzen und Producte der Variablen durch je eine Variable ersetzt werden. Daraus ergiebt sich auch als Corollar, dass jedes Functional ω in ein associirtes übergeht, wenn die Variablen irgendwie anders bezeichnet werden.

Es ist nun der folgende wichtige Satz zu beweisen:

3. Ist ω ein beliebiges ganzes Functional, so kann man eine durch ω theilbare Zahl α so wählen, dass der Quotient $\alpha : \omega$ zu einem beliebig gegebenen Functionale μ relativ prim ist.

Wir beweisen zunächst, dass es eine ganze Zahl α giebt, die durch ω, aber nicht durch $\omega\,\pi$ theilbar ist, wenn π ein beliebiges Primfunctional ist.

Bilden wir nämlich nach §. 142, 4. eine mit ω associirte ganze Function φ, so sind die Coëfficienten dieser Function zwar alle durch ω, aber nicht alle durch $\omega\,\pi$ theilbar, weil sonst auch φ und mithin ω selbst durch $\omega\,\pi$ theilbar wäre, was nicht möglich ist. Es giebt also unter den Coëfficienten von φ wenigstens einen, der die verlangte Eigenschaft hat.

Es sei jetzt $\pi_1, \pi_2, \pi_3, \ldots$ eine beliebige Anzahl von einander verschiedener gegebener Primfunctionale. Wir setzen

$$\omega_1 = \omega\,\pi_2\,\pi_3\,\ldots,\ \omega_2 = \omega\,\pi_1\,\pi_3\,\ldots,\ \omega_3 = \omega\,\pi_1\,\pi_2\,\ldots,$$

und bestimmen nach dem, was soeben bewiesen ist, die ganzen Zahlen $\alpha_1, \alpha_2, \alpha_3, \ldots$ in Ω, so dass

α_1 theilbar wird durch ω_1, aber nicht durch $\omega_1\,\pi_1$
α_2 „ „ „ ω_2 „ „ „ $\omega_2\,\pi_2$
α_3 „ „ „ ω_3 „ „ „ $\omega_3\,\pi_3$
. . . .,

und leiten daraus die ganze Zahl

$$\alpha = \alpha_1 + \alpha_2 + \alpha_3 + \cdots$$

ab. Diese Zahl ist offenbar theilbar durch ω, da alle Summanden $\alpha_1, \alpha_2, \alpha_3, \ldots$ durch ω theilbar sind. Sie ist aber nicht theilbar durch $\omega\,\pi_1$, weil zwar $\alpha_2, \alpha_3, \ldots$, nicht aber α_1 durch $\omega\,\pi_1$ theilbar ist; und ebenso ist sie nicht durch $\omega\,\pi_2$, $\omega\,\pi_3, \ldots$ theilbar. Wenn wir also

$$\alpha = \omega\,\eta$$

setzen, so ist η ein ganzes Functional, das nicht durch $\pi_1, \pi_2, \pi_3, \ldots$ theilbar ist, und das daher, wenn $\pi_1, \pi_2, \pi_3, \ldots$ die von einander verschiedenen Primfactoren von μ sind, relativ prim zu μ ist.

Nehmen wir nun beliebig eine durch ω theilbare ganze Zahl β in Ω an und setzen $\beta = \omega\,\mu$, dann können wir $\alpha = \omega\,\eta$ so bestimmen, dass η relativ prim zu μ wird, und dann ist ω der grösste gemeinschaftliche Theiler von α und β. Daraus folgt:

4. Jedes ganze Functional ω des Körpers Ω ist der grösste gemeinschaftliche Theiler zweier ganzer Zahlen, und folglich ist ω associirt mit einer binären Linearform $\alpha x + \beta y$, in der α und β ganze Zahlen sind.

Es mag hier noch eine allgemeine, auf ein anderes Gebiet hinübergreifende Bemerkung ihren Platz finden.

Es ist das Hauptergebniss dieses Abschnittes, dass sich die ganzen algebraischen Zahlen in einem bestimmten Körper in eindeutiger Weise in Primfactoren zerlegen lassen, genau in derselben Weise, wie dies bei den ganzen rationalen Zahlen bekannt ist; freilich aber nur dadurch, dass der Inhalt des Körpers

(durch Adjunction von Variablen) vergrössert wird. Es entsteht so ein erweiterter Körper, in dem die Gesetze der Zerlegbarkeit rein gelten.

Den Ausgangspunkt der Definitionen bildete der Körper R der rationalen Zahlen, und wenn wir uns Rechenschaft darüber geben wollen, auf welchen Eigenschaften des Körpers R die Möglichkeit dieser Erweiterung beruht, so finden wir, dass es einerseits die Existenz der ganzen Zahlen in R, andererseits die eindeutige Zerlegbarkeit dieser ganzen Zahlen in Primfactoren ist, die allein bei der ganzen Deduction benutzt wurden. Wenn wir also an Stelle des Körpers R irgend einen anderen Körper treten lassen, dem diese beiden Eigenschaften zukommen, so werden wir dieselben Folgerungen ziehen können. Nehmen wir für R einen anderen algebraischen Zahlkörper, so bekommen wir freilich nichts Neues, wohl aber, wenn wir z. B. an Stelle des Körpers R den Körper der rationalen Functionen einer Variablen setzen, dem ja die beiden fundamentalen Eigenschaften auch zukommen. So gewinnen wir einen Ausgangspunkt für die Theorie der algebraischen Functionen einer Variablen [1]).

[1]) Vergl. Dedekind-Weber, Theorie der algebraischen Functionen einer Veränderlichen. Crelle's Journal, Bd. 92.

Siebzehnter Abschnitt.

Theorie der algebraischen Körper.

---

§. 144.

Basis eines algebraischen Zahlkörpers. Discriminanten.

Es sei

(1) $$f(\Theta) = \Theta^n + a_1 \Theta^{n-1} + \cdots + a_n = 0$$

die irreducible Gleichung n^{ten} Grades mit rationalen Coëfficienten $a_1, a_2, \ldots, a_n$, die uns einen algebraischen Körper $\Omega = R(\Theta)$ definirt. Der Körper Ω ist dann der Inbegriff aller Zahlen der Form

(2) $$\omega = h_1 + h_2 \Theta + h_3 \Theta^2 + \cdots + h_n \Theta^{n-1},$$

worin $h_1, h_2, \ldots, h_n$ rationale Zahlen sind. Setzen wir aber für $h_1, h_2, \ldots, h_n$ rationale Functionale, so erhalten wir aus (2) alle Functionale des Körpers Ω.

Betrachten wir ein beliebiges System von n Zahlen

(3) $$\omega_r = h_{1,r} + h_{2,r} \Theta + \ldots + h_{n,r} \Theta^{n-1}, \quad r = 1, 2, \ldots, n$$

unter der Voraussetzung, dass die Determinante

(4) $$H = \Sigma \pm h_{1,1} h_{2,2} \ldots h_{n,n}$$

von Null verschieden ist, so kann, wegen der Irreducibilität von f, eine Gleichung der Form

(5) $$k_1 \omega_1 + k_2 \omega_2 + \cdots + k_n \omega_n = 0,$$

in der $k_1, k_2, \ldots, k_n$ rationale Zahlen sind, nur dann bestehen, wenn diese Coëfficienten alle Null sind, und dies gilt auch dann noch, wenn in der Gleichung (5) für die Coëfficienten rationale Functionale zugelassen werden.

Eliminiren wir aber aus den Gleichungen (2) und (3) die Potenzen von Θ, so ergiebt sich eine Relation von der Form

(6) $$\omega = k_1 \omega_1 + k_2 \omega_2 + \cdots + k_n \omega_n.$$

Man kann also jede Zahl und jedes Functional des Körpers Ω in der Form (6) darstellen, wenn man für $k_1, k_2, \ldots, k_n$ rationale Zahlen oder Functionale setzt. Diese Darstellung ist für ein gegebenes ω [wegen (5)] nur auf eine Art möglich, und ω ist eine Zahl, wenn die $k_1, k_2, \ldots, k_n$ Zahlen sind, dagegen ein Functional, wenn unter den k auch Functionale vorkommen.

Ein solches System von Zahlen, wie

$$\omega_1, \omega_2, \ldots, \omega_n,$$

nennen wir eine Basis des Körpers Ω. Eine solche Basis bilden auch die Potenzen von Θ:

$$1, \Theta, \Theta^2, \ldots, \Theta^{n-1}.$$

Bezeichnen wir mit $\omega_{r,1}, \omega_{r,2}, \ldots, \omega_{r,n}$ die mit ω_r conjugirten Zahlen, so ist das Determinantenquadrat

(7) $$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = (\Sigma \pm \omega_{1,1}\, \omega_{2,2} \ldots \omega_{n,n})^2$$

eine symmetrische Function der conjugirten Werthe $\Theta_1, \Theta_2, \ldots, \Theta_n$ und ist folglich eine rationale Zahl.

Diese Zahl heisst die Discriminante des Systemes $\omega_1, \omega_2, \ldots, \omega_n$. Insbesondere ist

(8) $$\Delta(1, \Theta, \Theta^2, \ldots, \Theta^{n-1}) = \begin{vmatrix} 1, \Theta_1, \ldots, \Theta_1^{n-1} \\ 1, \Theta_2, \ldots, \Theta_2^{n-1} \\ \cdots\cdots\cdots \\ 1, \Theta_n, \ldots, \Theta_n^{n-1} \end{vmatrix}^2$$

die Discriminante der Gleichung (1) (Bd. I, §. 46), für die man auch, wenn N das Zeichen für die Norm ist,

(9) $$(-1)^{\frac{n(n-1)}{2}}\, N f'(\Theta)$$

setzen kann. Diese Zahl ist also sicher von Null verschieden. Nach dem Multiplicationssatze der Determinanten (Bd. I, §. 27) ergiebt sich aus (3) und (7):

(10) $$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = H^2 \Delta(1, \Theta, \Theta^2, \ldots, \Theta^{n-1}),$$

woraus man schliesst, dass die Discriminante einer Basis von Ω immer von Null verschieden ist. Da H eine rationale Zahl ist, so folgt, dass das Verhältniss der Discriminanten verschiedener Basen das Quadrat einer rationalen Zahl ist, und dass die

Discriminanten aller Basen von Ω dasselbe Vorzeichen haben. Die Formel (10) zeigt auch, dass irgend ein System von n Zahlen ω_r des Körpers Ω immer dann eine Basis von Ω ist, wenn das Determinantenquadrat (7) nicht verschwindet.

Ist $\omega_1, \omega_2, \ldots, \omega_n$ eine Basis von Ω, und bedeuten $c_{r,s}$ rationale Zahlen, so bilden auch die n Zahlen

$$\omega'_r = c_{r,1}\omega_1 + c_{r,2}\omega_2 + \cdots + c_{r,n}\omega_n \qquad r = 1, 2, \ldots, n$$

eine Basis von Ω, wenn die Determinante

$$C = \Sigma \pm c_{1,1}c_{2,2}\ldots c_{n,n}$$

nicht verschwindet, und es ist

$$(11) \qquad \Delta(\omega'_1, \omega'_2, \ldots, \omega'_n) = C^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

Wenn wir z. B. die Elemente $\omega_1, \omega_2, \ldots, \omega_n$ einer Basis mit rationalen Coëfficienten $c_1, c_2, \ldots, c_n$ multipliciren, deren keiner verschwindet, so erhalten wir eine neue Basis

$$c_1\omega_1,\ c_2\omega_2, \ldots, c_n\omega_n.$$

§. 145.

Die Minimalbasis und die Körperdiscriminante.

Nach der zuletzt gemachten Bemerkung verliert eine Basis von Ω die Eigenschaft, eine Basis zu sein, nicht, wenn man jede ihrer Zahlen mit einer von Null verschiedenen rationalen Zahl multiplicirt. Nun kann man nach §. 133, 5. jede Zahl durch Multiplication mit einer ganzen rationalen Zahl in eine ganze Zahl verwandeln, und daraus folgt, dass es Basen von Ω giebt, deren Elemente lauter ganze Zahlen sind. Die Discriminante einer solchen Basis ist eine ganze rationale Zahl. Diese ganze rationale Zahl ist von Null verschieden. Sie ändert sich, wenn eine andere ganzzahlige Basis gewählt wird, behält aber für einen bestimmten Körper ein unverändertes Vorzeichen.

Unter all diesen ganzen Zahlen, die als Discriminanten einer ganzzahligen Basis auftreten können, und die alle in quadratischem Verhältniss zu einander stehen, muss nun eine dem absoluten Werthe nach die kleinste sein. Diese kleinste Discriminante bezeichnen wir mit Δ und nennen sie die Grundzahl oder auch die Discriminante des Körpers Ω.

Dies Δ ist eine durch Ω völlig bestimmte positive oder negative, aber niemals verschwindende ganze rationale Zahl, und es giebt immer eine aus ganzen Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ bestehende Basis von Ω, deren Discriminante gleich Δ ist.

Eine solche Basis wollen wir kurz eine **Minimalbasis von Ω** nennen.

Verstehen wir unter $k_1, k_2, \ldots, k_n$ irgend welche ganze rationale Zahlen, so ist jede Zahl von der Gestalt

$$(1) \qquad \omega = k_1 \omega_1 + k_2 \omega_2 + \cdots + k_n \omega_n$$

eine ganze algebraische Zahl, und wir beweisen jetzt den fundamentalen Satz:

1. Wenn $\omega_1, \omega_2, \ldots, \omega_n$ eine Minimalbasis ist, so sind in der Form (1) alle ganzen Zahlen des Körpers Ω enthalten.

Da $\omega_1, \omega_2, \ldots, \omega_n$ eine Basis ist, so kann zunächst jede Zahl in Ω in der Form (1) dargestellt werden, wenn für $k_1, k_2, \ldots, k_n$ rationale Brüche zugelassen werden. Nehmen wir also an, es sei eine ganze Zahl ω in der Form

$$(2) \qquad \omega = \frac{k_1 \omega_1 + k_2 \omega_2 + \cdots + k_n \omega_n}{k}$$

darstellbar, worin $k_1, k_2, \ldots, k_n, k$ ganze rationale Zahlen sind, so dass nicht alle $k_1, k_2, \ldots, k_n$ mit k einen gemeinschaftlichen Theiler haben. Ist p irgend eine in k aufgehende natürliche Primzahl und $k = p k'$, so muss wenigstens einer der Coëfficienten $k_1, k_2, \ldots, k_n$ durch p untheilbar sein. Es sei etwa k_1 durch p nicht theilbar; dann lässt sich die ganze rationale Zahl l so bestimmen, dass $l k_1 \equiv 1 \pmod{p}$, oder $(l k_1 - 1)$ durch p theilbar wird. Es folgt dann aus (2):

$$(3) \qquad l k' \omega - \frac{l k_1 - 1}{p} \omega_1 = \frac{\omega_1 + l k_2 \omega_2 + \cdots + l k_n \omega_n}{p} = \omega_1',$$

und ω_1' ist gleichfalls eine ganze algebraische Zahl. Setzen wir

$$(4) \qquad \omega_2' = \omega_2, \ldots, \omega_n' = \omega_n,$$

so bilden die Zahlen $\omega_1', \omega_2', \ldots, \omega_n'$ eine ganzzahlige Basis von Ω, weil sich die Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ und folglich alle Zahlen ω linear durch $\omega_1', \omega_2', \ldots, \omega_n'$ ausdrücken lassen, und die Formel (11) des vorigen Paragraphen ergiebt

$$(5) \qquad \Delta(\omega_1', \omega_2', \ldots, \omega_n') = \frac{1}{p^2} \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

Die Discriminante $\Delta(\omega_1', \omega_2', \ldots, \omega_n')$ ist also kleiner als $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$, und dies widerspricht der Annahme, dass $\omega_1, \omega_2, \ldots, \omega_n$ eine Minimalbasis sei. Damit ist unser Satz erwiesen.

Bezeichnet man die Gesammtheit aller ganzen Zahlen des Körpers Ω mit $\mathfrak{o}$, so erhält man alle Zahlen von $\mathfrak{o}$, und jede nur einmal, wenn man in

(6) $$k_1 \omega_1 + k_2 \omega_2 + \cdots + k_n \omega_n$$

die Coefficienten $k_1, k_2, \ldots, k_n$ die sämmtlichen ganzen rationalen Zahlen durchlaufen lässt.

Aus diesem Grunde wird eine Minimalbasis von Ω auch eine Basis von $\mathfrak{o}$ genannt.

Die Discriminante einer Basis von $\mathfrak{o}$ ist gleich der Grundzahl des Körpers Ω.

Nach der Formel (11) des vorigen Paragraphen können wir aus einer Basis von $\mathfrak{o}$ beliebig viele andere durch lineare Substitution ableiten:

(7) $$(\omega_1', \omega_2', \ldots, \omega_n') = C(\omega_1, \omega_2, \ldots, \omega_n),$$

wenn C (nach den Bezeichnungen des §. 37) eine lineare Substitution mit rationalen ganzzahligen Coëfficienten und der Determinante ± 1 bedeutet.

Da nach der Bedeutung der Basis von $\mathfrak{o}$ alle ganzen Zahlen in Ω, also auch die Elemente $\omega_1', \omega_2', \ldots, \omega_n'$ einer zweiten Basis von $\mathfrak{o}$ linear mit ganzen rationalen Coëfficienten durch $\omega_1, \omega_2, \ldots, \omega_n$ darstellbar sind, so folgt auch umgekehrt, dass man durch solche lineare Substitutionen mit der Determinante ± 1 aus einer Basis von $\mathfrak{o}$ alle anderen ableiten kann.

Denn ist

$$(\omega_1, \omega_2, \ldots, \omega_n) = C'(\omega_1', \omega_2', \ldots, \omega_n'),$$

so muss die zusammengesetzte Substitution $C C'$ die identische sein, und das Product beider Determinanten ist also 1, also jede von ihnen $= \pm 1$.

Da unter den Zahlen von $\mathfrak{o}$ immer die Zahl 1 enthalten ist, so kann man, wenn $\omega_1, \omega_2, \ldots, \omega_n$ eine Basis von $\mathfrak{o}$ ist, die ganzen rationalen Zahlen $c_1, c_2, \ldots, c_n$ so bestimmen, dass die Relation

(8) $$c_1 \omega_1 + c_2 \omega_2 + \cdots + c_n \omega_n = 1$$

befriedigt ist.

Es gilt aber auch in Bezug auf die Functionale der Satz:

2. **Wenn $\omega_1, \omega_2, \ldots, \omega_n$ eine Basis von $\mathfrak{o}$ ist, so sind in der Form**

(9) $$\omega = u_1 \omega_1 + u_2 \omega_2 + \cdots + u_n \omega_n,$$

in der $u_1, u_2, \ldots, u_n$ ganze rationale Functionale sind, alle ganzen Functionale in Ω enthalten.

Denn wir haben schon oben gezeigt, dass alle Functionale überhaupt in der Form (9) enthalten sind, wenn die Coëfficienten $u_1, u_2, \ldots, u_n$ ganze oder gebrochene rationale Functionale sind. Wir können aber immer eine ganze primitive Function e so bestimmen, dass

$$e u_1 = y_1, \; e u_2 = y_2, \ldots, e u_n = y_n$$

ganze Functionen der Variablen sind, und dann wird

(10) $$e \omega = y_1 \omega_1 + y_2 \omega_2 + \cdots + y_n \omega_n,$$

und da e eine Einheit ist, so ist $e\omega$ zugleich mit ω ganz. Da nun die Coëfficienten der Potenzen und Producte der Variablen in der Function (10) nach §. 142, 3. ganze Zahlen sein müssen, so folgt nach 1., dass die Coëfficienten in den Functionen $y_1, y_2, \ldots, y_n$ ganze rationale Zahlen sein müssen, und dass folglich $u_1, u_2, \ldots, u_n$ ganze rationale Functionale sind.

§. 146.

Die Basen der Functionale.

Ist μ ein ganzes Functional des Körpers Ω, so verstehen wir unter einer Basis von μ ein System von n ganzen Zahlen in Ω:

(1) $$\alpha_1, \alpha_2, \ldots, \alpha_n,$$

das eine Basis des Körpers Ω ist, und dem die Eigenschaft zukommt, dass in der Form

(2) $$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n$$

alle durch μ theilbaren ganzen Zahlen des Körpers Ω und keine anderen enthalten sind, wenn für $x_1, x_2, \ldots, x_n$ ganze rationale Zahlen gesetzt werden.

Es soll jetzt bewiesen werden, dass jedes ganze Functional eine Basis hat.

Zunächst ist klar, dass eine Basis eines Functionals μ zugleich Basis aller mit μ associirten Functionale ist, ferner dass jedes Element $\alpha_1, \alpha_2, \ldots$ einer solchen Basis durch μ theilbar sein muss, endlich dass aus einer Basis von μ alle anderen abgeleitet werden können, wenn man eine lineare Substitution mit ganzen rationalen Coëfficienten und der Determinante ± 1 anwendet.

Um nun eine Basis von μ zu bilden, gehen wir von einer Minimalbasis (Basis von $\mathfrak{o}$) aus, die wir, wie oben, mit

$$\omega_1, \omega_2, \ldots, \omega_n$$

bezeichnen.

Da es positive ganze rationale Zahlen giebt, die durch μ theilbar sind, so giebt es auch ganze rationale Zahlen a, für die das Product $a\,\omega_1$ durch μ theilbar ist. Die **kleinste** positive unter diesen Zahlen wollen wir mit $a_{1,1}$ bezeichnen und

$$\alpha_1 = a_{1,1}\,\omega_1$$

setzen. Sodann bezeichnen wir mit $a_{2,2}$ die **kleinste** positive ganze rationale Zahl, für die sich ein ganzes rationales $a_{1,2}$ so bestimmen lässt, dass

$$\alpha_2 = a_{1,2}\,\omega_1 + a_{2,2}\,\omega_2$$

durch μ theilbar wird, und fahren so fort. Wir bilden auf diese Weise das System

$$(3)\qquad \begin{aligned} \alpha_1 &= a_{1,1}\,\omega_1 \\ \alpha_2 &= a_{1,2}\,\omega_1 + a_{2,2}\,\omega_2 \\ &\ldots\ldots\ldots\ldots\ldots \\ \alpha_n &= a_{1,n}\,\omega_1 + a_{2,n}\,\omega_2 + \cdots + a_{n,n}\,\omega_n, \end{aligned}$$

worin $a_{1,1}, a_{2,2}, \ldots, a_{n,n}$ die kleinsten positiven ganzen rationalen Zahlen sind, die eine Bestimmung der ganzen rationalen Zahlen $a_{1,2}, \ldots, a_{n-1,n}$ so ermöglichen, dass die ganzen Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ durch μ theilbar werden.

Jede Zahl $a_{r,r}$ ist hiernach unabhängig von den übrigen dadurch definirt, dass sie die kleinste natürliche Zahl ist, für die sich die zugehörigen ganzen rationalen Zahlen $a_{1,r}, a_{2,r}, \ldots, a_{r-1,r}$ so bestimmen lassen, dass

$$(4)\qquad \alpha_r = a_{1,r}\,\omega_1 + a_{2,r}\,\omega_2 + \cdots + a_{r-1,r}\,\omega_{r-1} + a_{r,r}\,\omega_r$$

durch μ theilbar wird. In dem besonderen Falle, wo ω_r selbst durch μ theilbar ist, hat man demnach $a_{r,r} = 1$ zu setzen, und

die $a_{1,r}, a_{2,r}, \ldots, a_{r-1,r}$ können alle gleich Null angenommen werden.

Bezeichnen wir mit Δ die Grundzahl des Körpers Ω, so ergiebt sich die Discriminante des durch (3) bestimmten Systemes $\alpha_1, \alpha_2, \ldots, \alpha_n$ nach der Formel §. 144, (11):

(5) $$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = a_{1,1}^2 a_{2,2}^2 \ldots a_{n,n}^2 \Delta.$$

Dies ist eine von Null verschiedene ganze rationale Zahl, und folglich sind die Grössen α eine Basis von Ω.

Um also zu zeigen, dass das so bestimmte System $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine Basis von μ ist, bleibt noch nachzuweisen, dass jede durch μ theilbare ganze Zahl α in der Form (2) dargestellt werden kann. Nehmen wir, um diesen Beweis zu führen, irgend einen Index $r \gtreqless n$ an, und suchen die Bedingung dafür, dass eine ganze Zahl von der Form

(6) $$\gamma_r = h_1 \omega_1 + h_2 \omega_2 + \cdots + h_r \omega_r$$

durch μ theilbar ist, wenn $h_1, h_2, \ldots, h_r$ ganze rationale Zahlen sind.

Zunächst folgt, dass h_r durch $a_{r,r}$ theilbar sein muss. Denn bezeichnen wir mit q_r den Rest der Division von h_r durch $a_{r,r}$, und setzen

$$h_r = l_r a_{r,r} + q_r, \quad 0 \gtreqless q_r < a_{r,r},$$

so ergiebt sich nach (6)

$$\gamma_r - l_r \alpha_r = (h_1 - l_r a_{1,r}) \omega_1 + (h_2 - l_r a_{2,r}) \omega_2 + \cdots + q_r \omega_r,$$

und diese Zahl müsste auch durch μ theilbar sein. Dies ist aber nach der Definition von $a_{r,r}$ nur möglich, wenn $q_r = 0$ ist. Dann aber erhält $\gamma_r - l_r \alpha_r$ den Ausdruck:

(7) $$\gamma_r - l_r \alpha_r = h_1' \omega_1 + h_1' \omega_2 + \cdots + h_{r-1}' \omega_{r-1},$$

wird also von derselben Form, wie (6), nur dass $r - 1$ an Stelle von r tritt, und in (7) ist dieselbe Schlussweise zu wiederholen. Demnach ergiebt sich durch vollständige Induction der Satz:

Eine in der Form $h_1 \omega_1 + h_2 \omega_2 + \cdots + h_r \omega_r$ darstellbare ganze Zahl des Körpers Ω ist immer dann und nur dann durch μ theilbar, wenn sie in der Form

$$l_1 \alpha_1 + l_2 \alpha_2 + \cdots + l_r \alpha_r$$

darstellbar ist, in der die Coëfficienten $l_1, l_2, \ldots, l_r$ ganze rationale Zahlen sind.

Setzt man in diesem Satze $r = n$, so hat man den Beweis dafür, dass das Zahlensystem (3) eine Basis von μ ist.

Wie man aus der einen Basis von μ alle anderen ableiten kann, haben wir schon oben gesehen.

Wir verstehen jetzt unter $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine beliebige Basis von μ und stellen das Functional μ nach §. 142, 4. als Quotienten zweier ganzer Functionen dar, dessen Nenner eine rationale Einheit ist. Die Coëfficienten des Zählers sind dann ganze durch μ theilbare Zahlen (§. 143, 2.) und können daher in der Form (2) dargestellt werden.

Fassen wir diese Darstellung gehörig zusammen, so ergiebt sich also für μ ein Ausdruck

$$(8) \qquad \mu = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n,$$

worin die $u_1, u_2, \ldots, u_n$ ganze rationale Functionale sind.

Hiermit wollen wir die Linearform

$$(9) \qquad \lambda = \alpha_1 t_1 + \alpha_2 t_2 + \cdots + \alpha_n t_n$$

vergleichen, in der $t_1, t_2, \ldots, t_n$ Variable sind. Diese Linearform ist (nach §. 139) der grösste gemeinschaftliche Theiler der Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ und ist durch μ theilbar, weil die Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ durch μ theilbar sind. Andererseits ist aber auch, wie die Darstellung (8) zeigt, μ durch λ theilbar, und folglich sind die beiden Functionale μ und λ mit einander associirt.

Das Functional λ wollen wir eine Basisform des Functionals μ nennen; es ist dann λ zugleich Basisform von allen mit μ associirten Functionalen.

Eine Basisform λ von μ hat die Eigenschaft, dass man aus ihr alle durch μ (oder durch λ) theilbaren ganzen Zahlen in Ω erhält, wenn man für die Variablen ganze rationale Zahlen setzt.

Die Basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ steht zu dem Functionale μ in einer ähnlichen Beziehung, wie die Basis $\omega_1, \omega_2, \ldots, \omega_n$ des Systemes $\mathfrak{o}$ aller ganzen Zahlen in Ω zu den Einheiten. In der That ist die Linearform

$$(10) \qquad \tau = \omega_1 t_1 + \omega_2 t_2 + \cdots + \omega_n t_n$$

eine Einheit; denn sie ist der grösste gemeinschaftliche Theiler von $\omega_1, \omega_2, \ldots, \omega_n$ und muss also, wie die Formel §. 145, (8) zeigt, ein Theiler von 1, also eine Einheit sein.

Demnach wollen wir das Functional τ eine Basisform von $\mathfrak{o}$ nennen.

Aus einer solchen Basisform erhält man alle ganzen Zahlen des Körpers Ω, wenn man für die Variablen ganze rationale Zahlen setzt.

Die Grundform τ ist die Wurzel einer irreduciblen Gleichung n^{ten} Grades

$$F(t) = N(t - \tau) = 0,$$

in der die Coëfficienten der Potenzen von t ganze rationale (und homogene) Functionen der Variablen $t_1, t_2, \ldots, t_n$ sind.

§. 147.

Die absoluten Normen der Functionale.

Die Elemente $\alpha_1, \alpha_2, \ldots, \alpha_n$ einer Basis des Functionals μ können als ganze Zahlen in Ω linear und ganzzahlig ausgedrückt werden durch eine Basis $\omega_1, \omega_2, \ldots, \omega_n$ von $\mathfrak{o}$ in der Form

(1) $$(\alpha_1, \alpha_2, \ldots, \alpha_n) = A\,(\omega_1, \omega_2, \ldots, \omega_n),$$

worin A eine lineare Substitution mit ganzen rationalen Coëfficienten bedeutet. Einen Specialfall hiervon bieten die Formeln (3) des vorigen Paragraphen.

Eine Basisform λ von μ wollen wir so darstellen:

(2) $$\lambda = \sum^{\nu} \alpha_\nu\, t_\nu,$$

und die Substitution (1) schreiben wir ausführlicher:

(3) $$\alpha_s = \sum^{\nu} a_{s,\nu}\, \omega_\nu,$$

worin t_ν Variable, $a_{s,\nu}$ die Substitutionscoëfficienten sind, und der Summationsbuchstabe ν von 1 bis n läuft.

Da die Producte $\alpha_s\,\omega_r$ alle durch μ theilbar sind, so können sie nach der Bedeutung der Basis in der Form dargestellt werden

(4) $$\alpha_\nu\, \omega_r = \sum^{s} g_{\nu,r}^{(s)}\, \alpha_s,$$

worin die $g_{\nu,r}^{(s)}$ ganze rationale Zahlen sind. Hieraus erhält man dann nach (2)

(5) $$\lambda\, \omega_r = \sum^{s} \alpha_s\, t_{s,r},$$

wenn

(6) $$t_{s,r} = \sum^{\nu} g_{\nu,r}^{(s)}\, t_\nu$$

ganze rationale Linearformen sind.

Substituirt man in (5) wieder die Ausdrücke (3), so folgt

(7) $$\lambda\, \omega_r = \sum^{\nu} \omega_\nu \sum^{s} a_{s,\nu}\, t_{s,r}.$$

Eliminiren wir aus diesen linearen Gleichungen die ω_ν, so können wir die Gleichung n^{ten} Grades für λ in Determinantenform darstellen, und das Product der Wurzeln dieser Gleichung, also die Norm von λ, erhalten wir als die Determinante aus den n^2 Grössen

$$\sum^{s} a_{s,\nu}\, t_{s,r}$$

(§. 137, 8.). Diese Determinante lässt sich aber nach dem Multiplicationssatze der Determinanten (s. Bd. I, §. 27) zerlegen, und giebt, wenn

$$A = \Sigma \pm a_{1,1}\, a_{2,2} \ldots a_{n,n}, \quad T = \Sigma \pm t_{1,1}\, t_{2,2} \ldots t_{n,n}$$

gesetzt wird,

(8) $$N(\lambda) = A\,T.$$

Hierin ist T eine ganze Function der Variablen t_ν mit ganzen rationalen Zahlencoëfficienten, von der wir nun noch nachweisen werden, dass sie primitiv ist.

Nehmen wir an, im Theiler von T gehe irgend eine natürliche Primzahl p auf. Dann können wir n ganze rationale Formen $y_1, y_2, \ldots, y_n$ der Variablen t so bestimmen, dass die n Summen

(9) $$u_s = t_{s,1}\, y_1 + t_{s,2}\, y_2 + \cdots + t_{s,n}\, y_n$$

alle durch p theilbar sind, ohne dass alle $y_1, y_2, \ldots, y_n$ durch p theilbar sind.

Die Richtigkeit dieser Behauptung folgt aus elementaren Determinantensätzen (Bd. I, zweiter Abschnitt).

Wenn nämlich die $t_{s,r}$ alle durch p theilbar sind, so können wir die y_r ganz beliebig z. B. gleich 1 annehmen.

Andernfalls nehmen wir an, dass ausser der Determinante T auch alle m-reihigen Unterdeterminanten durch p theilbar seien ($m \gtreqless n$), und dass unter den $(m-1)$-reihigen Unterdeterminanten wenigstens eine nicht durch p theilbar sei. Ist dann etwa unter den $(m-1)$-reihigen Determinanten der Matrix

$$\begin{matrix} t_{1,1}, & t_{1,2}, & \ldots, & t_{1,m} \\ \cdots & \cdots & \cdots & \cdots \\ t_{m-1,1}, & t_{m-1,2}, & \ldots, & t_{m-1,m} \end{matrix}$$

eine durch p nicht theilbar, so setzen wir für $y_1, y_2, \ldots, y_m$ eben diese $(m-1)$-reihigen Determinanten und nehmen $y_{m+1}, \ldots, y_n = 0$ an. Diese y genügen dann der gestellten Forderung.

Sind die y dann so bestimmt, so setzen wir

(10) $$\omega = \omega_1 y_1 + \omega_2 y_2 + \cdots + \omega_n y_n,$$

und leiten aus (5) die Gleichung ab

(11) $$\lambda \omega = \sum^{s} \alpha_s u_s.$$

Da nun die α_s durch λ und die u_s durch p theilbar sind, so folgt, dass ω durch p theilbar ist, und dass mithin, nach §. 145, 2., $y_1, y_2, \ldots, y_n$ durch p theilbar sein müssen, was unserer Voraussetzung entgegen ist.

Damit ist bewiesen, dass T eine primitive Function ist, und dass also der absolute Werth der Determinante A gleich der absoluten Norm von λ und folglich auch von μ ist (§. 138).

Wenden wir das Ergebniss auf die specielle Basis (3), §. 146 an, so ergiebt sich die Formel:

(12) $$N_a(\mu) = a_{1,1}\, a_{2,2} \ldots a_{n,n}.$$

Hieran knüpfen wir noch folgende Bemerkungen: Wenn man in einer Basisform eines Functionales μ

$$\lambda = \alpha_1 t_1 + \alpha_2 t_2 + \cdots + \alpha_n t_n$$

auf die Variablen $t_1, t_2, \ldots, t_n$ eine ganzzahlige lineare Substitution mit der Determinante ± 1 anwendet, so entsteht eine neue Basisform von μ. Denn allen ganzzahligen rationalen Werthen der Variablen $t_1, t_2, \ldots, t_n$ entsprechen ganzzahlige rationale Werthe der neuen Variablen und umgekehrt.

Die Anwendung einer linearen Substitution auf die Variablen t ist aber gleichbedeutend mit der Anwendung der transponirten Substitution auf die Coëfficienten $\alpha_1, \alpha_2, \ldots, \alpha_n$ (§. 37), d. h. mit dem Uebergange zu einer neuen Basis von μ:

(13) $$(\beta_1, \beta_2, \ldots, \beta_n) = (B)\,(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

die dann durch Zusammensetzung mit (1) ergiebt:

(14) $$(\beta_1, \beta_2, \ldots, \beta_n) = (B)\,(A)\,(\omega_1, \omega_2, \ldots, \omega_n).$$

Wenn die Discriminante (§. 144) der durch eine Substitution (13) bestimmten Zahlen β mit der Discriminante der α übereinstimmt, so muss die Substitutionsdeterminante $B = \pm 1$ sein; und wir kommen also zu den Sätzen:

1. Die Discriminante einer Basis von μ ist gleich dem Quadrate der absoluten Norm von μ, multiplicirt mit der Grundzahl des Körpers;

und umgekehrt:

2. Ist $\beta_1, \beta_2, \ldots, \beta_n$ ein System ganzer durch μ theilbarer Zahlen, dessen Discriminante gleich ist dem Quadrate der absoluten Norm von μ, multiplicirt mit der Grundzahl des Körpers, so ist $\beta_1, \beta_2, \ldots, \beta_n$ eine Basis von μ.

§. 148.

Volles Restsystem nach einem Modul.

1. **Definition:** Zwei ganze algebraische Zahlen ξ, η, deren Differenz $\xi - \eta$ durch ein ganzes von Null verschiedenes Functional μ theilbar ist, heissen mit einander congruent nach dem Modul μ.

Der Begriff der Congruenz lässt sich auch auf Functionale ausdehnen, was wir aber fürs Erste noch nicht thun. Dagegen ist es wesentlich, als Moduln der Congruenz nicht bloss die Zahlen, sondern auch die Functionale zu berücksichtigen. Jede Congruenz bleibt bestehen, wenn der Modul durch ein associirtes Functional ersetzt wird. Beim Modul können beliebige Einheitsfactoren hinzugefügt oder weggelassen werden.

Wir gebrauchen für die Congruenz das Gauss'sche Zeichen (Bd. I, §. 115)

(1) $$\xi \equiv \eta \pmod{\mu}.$$

Eine solche Congruenz ist gleichbedeutend mit der Gleichung

(2) $$\xi = \eta + \omega \mu,$$

worin ω irgend ein ganzes Functional sein kann.

Aus dieser Darstellung erkennt man dann sofort, dass, ebenso wie in Congruenzen zwischen rationalen Zahlen, wenn man in einem durch Addition, Subtraction und Multiplication von ganzen Zahlen zusammengesetzten Ausdruck jede Zahl durch eine nach dem Modul μ congruente Zahl ersetzt, eine nach demselben Modul congruente Zahl das Resultat ist; in Zeichen:

Sind $\xi_1, \eta_1, \xi_2, \eta_2, \ldots$ ganze Zahlen, die den Congruenzen

$$\xi_1 \equiv \eta_1, \ \xi_2 \equiv \eta_2, \ldots \pmod{\mu}$$

genügen, und ist $\psi(x_1, x_2, \ldots)$ eine ganze Function mit ganzzahligen rationalen Coëfficienten, so ist auch

$$(3) \qquad \psi(\xi_1, \xi_2, \ldots) \equiv \psi(\eta_1, \eta_2, \ldots) \pmod{\mu}.$$

2. **Ist m die kleinste positive ganze rationale Zahl, die durch μ theilbar ist, so sind zwei nach dem Modul μ congruente ganze rationale Zahlen auch nach dem Modul m congruent** (§. 138, 13.).

Ein Hauptsatz über die Congruenzen, zu dessen Beweis wir jetzt schreiten, ist der:

3. **Die Anzahl der nach einem Modul μ incongruenten ganzen Zahlen eines Körpers Ω ist endlich, und zwar gleich der absoluten Norm von μ.**

Um ihn zu beweisen, nehmen wir eine Basis des Functionals μ an, und zwar wählen wir gerade die im §. 146, (3) bestimmte specielle Basis:

$$(4) \qquad \begin{array}{l} \alpha_1 = a_{1,1}\,\omega_1 \\ \alpha_2 = a_{1,2}\,\omega_1 + a_{2,2}\,\omega_2 \\ \cdots\cdots\cdots\cdots\cdots \\ \alpha_n = a_{1,n}\,\omega_1 + a_{2,n}\,\omega_2 + \cdots + a_{n,n}\,\omega_n, \end{array}$$

worin $\omega_1, \omega_2, \ldots, \omega_n$ eine Basis von $\mathfrak{o}$ ist.

Jede ganze Zahl η in Ω lässt sich dann in der Form darstellen:

$$(5) \qquad \eta = y_1\,\omega_1 + y_2\,\omega_2 + \cdots + y_n\,\omega_n,$$

wenn die $y_1, y_2, \ldots, y_n$ ganze rationale Zahlen sind. Damit verbinden wir das Zahlensystem

$$(6) \qquad \xi = x_1\,\omega_1 + x_2\,\omega_2 + \cdots + x_n\,\omega_n,$$

in dem wir x_1 ein volles Restsystem nach dem Modul $a_{1,1}$, x_2 nach dem Modul $a_{2,2}, \ldots, x_n$ nach dem Modul $a_{n,n}$ durchlaufen lassen. Die Anzahl der so gebildeten Zahlen ξ beträgt $a_{1,1}\,a_{2,2} \ldots a_{n,n}$, eine Zahl, die nach §. 147, (12) gleich der absoluten Norm von μ ist.

Wir wollen nachweisen, dass jede Zahl η einer und nur einer dieser Zahlen ξ nach dem Modul μ congruent ist.

Wenn $\eta - \xi$ durch μ theilbar sein soll, so muss nach der Bedeutung der Basis diese Differenz in der Form

$$(7) \qquad \eta - \xi = h_1\,\alpha_1 + h_2\,\alpha_2 + \cdots + h_n\,\alpha_n$$

darstellbar sein, worin die $h_1, h_2, \ldots, h_n$ ganze rationale Zahlen sind, und wenn diese Bedingung erfüllt ist, so ist auch umgekehrt η mit ξ nach dem Modul μ congruent. Ordnen wir die rechte Seite mittelst (4) nach $\omega_1, \omega_2, \ldots, \omega_n$, so ergiebt sich aus (5) und (6):

$$(8)\quad \begin{aligned} y_1 &= x_1 + h_1 a_{1,1} + h_2 a_{1,2} + \cdots + h_n a_{1,n} \\ y_2 &= x_2 + \phantom{h_1 a_{1,1} +} h_2 a_{2,2} + \cdots + h_n a_{2,n} \\ &\cdots\cdots\cdots\cdots\cdots \\ y_n &= x_n \phantom{+ h_1 a_{1,1} + h_2 a_{2,2} + \cdots} + h_n a_{n,n}. \end{aligned}$$

Darin aber liegt der Beweis unserer Behauptung. Denn sind $y_1, y_2, \ldots, y_n$ irgend welche gegebene ganze rationale Zahlen, so ist zunächst aus

$$y_n = x_n + h_n a_{n,n}$$

x_n und h_n vollständig bestimmt. Darauf erhalten wir aus der vorletzten Gleichung

$$y_{n-1} - h_n a_{n-1,n} = x_{n-1} + h_{n-1} a_{n-1,n-1},$$

wodurch x_{n-1} und h_{n-1} völlig bestimmt sind. Die nächst vorhergehende Gleichung ergiebt

$$y_{n-2} - h_n a_{n-2,n} - h_{n-1} a_{n-2,n-1} = x_{n-2} + h_{n-2} a_{n-2,n-2},$$

wodurch x_{n-2} und h_{n-2} völlig bestimmt sind, und so fahren wir fort, bis alle x_i und h_i bestimmt sind.

Hiernach können wir zweckmässig die Gesammtheit der Zahlen ξ oder irgend ein System mit diesen congruenter Zahlen ein volles Restsystem nach dem Modul μ nennen.

Die Anzahl der Individuen eines vollen Restsystems für den Modul μ ist gleich der absoluten Norm von μ.

§. 149.

Congruenzen.

Aus der Existenz eines vollen Restsystems nach einem Modul μ, die wir im vorigen Paragraphen nachgewiesen haben, ergiebt sich eine Reihe von Sätzen, die mit bekannten elementaren Sätzen der rationalen Zahlentheorie analog sind.

Bedeutet α irgend eine ganze Zahl in Ω und μ ein als Modul dienendes ganzes Functional, und ist α relativ prim zu μ, so sind zwei Zahlen $\alpha\xi$ und $\alpha\xi'$ nur dann congruent nach dem

Modul μ, wenn die ganzen Zahlen ξ, ξ' congruent sind. Hieraus ergiebt sich, dass, wenn ξ ein volles Restsystem nach dem Modul μ durchläuft, dasselbe auch von dem Producte $\alpha\xi$ gilt, wodurch der Satz bewiesen ist:

1. Ist α eine ganze Zahl in Ω, relativ prim zu dem Modul μ, ferner γ eine beliebige ganze Zahl in Ω, so ist die Congruenz:

$$\alpha\xi \equiv \gamma \pmod{\mu} \tag{1}$$

immer durch eine ganze Zahl ξ lösbar, und auch nur durch eine, wenn für ξ ein volles Restsystem nach dem Modul μ vorgeschrieben ist.

Wenn hierin μ selbst eine Zahl ist, die wir mit β bezeichnen, so ist auch der Quotient

$$\frac{\alpha\xi - \gamma}{\beta} = -\eta$$

eine ganze Zahl, und dann nimmt der vorstehende Satz die Form an:

2. Sind α, β, γ drei ganze Zahlen in Ω und α, β relativ prim, so kann man zwei andere ganze Zahlen ξ, η in Ω so bestimmen, dass

$$\alpha\xi + \beta\eta = \gamma \tag{2}$$

wird. Insbesondere kann man also auch für zwei beliebige relative Primzahlen α, β die Gleichung

$$\alpha\xi + \beta\eta = 1 \tag{3}$$

durch ganze Zahlen ξ, η befriedigen.

Dieser Satz lässt sich auf ein System von mehreren Zahlen übertragen.

Wenn die Zahlen $\alpha, \beta, \gamma, \ldots$ in $\mathfrak{o}$ keinen gemeinsamen Theiler haben, so können wir zunächst Zahlen $\eta_1, \zeta_1, \ldots$ in $\mathfrak{o}$ so bestimmen, dass

$$\beta_1 = \beta\eta_1 + \gamma\zeta_1 + \cdots$$

relativ prim zu α wird. Wir haben nämlich, wenn $\pi_1, \pi_2, \ldots$ die verschiedenen Primfactoren von α sind, deren keiner in allen $\beta, \gamma, \ldots$ aufgehen kann, und wenn etwa β durch π_1 nicht theilbar ist, η_1 durch π_1 untheilbar, die übrigen Zahlen $\zeta_1, \ldots$ durch π_1 theilbar u. s. f. anzunehmen, und erhalten für jede der Zahlen $\eta_1, \zeta_1, \ldots$ die Bedingung, dass sie durch einige der Primfactoren

x_i theilbar, durch andere nicht theilbar sein soll, und dieser Forderung kann nach §. 143, 3. immer genügt werden. Dann können wir nach 2. die ganze Zahl τ so bestimmen, dass

$$\alpha\xi + \beta_1 \tau = 1$$

wird, und wenn wir $\tau\eta_1 = \eta$, $\tau\zeta_1 = \zeta, \ldots$ setzen, so erhalten wir den Satz:

3. Sind $\alpha, \beta, \gamma, \ldots$ Zahlen in $\mathfrak{o}$ ohne gemeinschaftlichen Theiler, so lassen sich andere Zahlen $\xi, \eta, \zeta, \ldots$ in $\mathfrak{o}$ so bestimmen, dass

(4) $$\alpha\xi + \beta\eta + \gamma\zeta + \cdots = 1$$

wird.

Daraus lässt sich weiter auf folgenden Satz schliessen:

4. Sind $\alpha, \beta, \gamma, \ldots$ beliebige Zahlen in $\mathfrak{o}$, μ eine durch den grössten gemeinschaftlichen Theiler aller dieser Zahlen theilbare Zahl in $\mathfrak{o}$, so kann man die Zahlen $\xi, \eta, \zeta, \ldots$ in $\mathfrak{o}$ so bestimmen, dass

(5) $$\mu = \alpha\xi + \beta\eta + \gamma\zeta + \cdots$$

wird.

Wenn wir nämlich den grössten gemeinschaftlichen Theiler der Zahlen $\alpha, \beta, \gamma, \ldots$ nach §. 139 in der Form

$$\delta = \alpha u + \beta v + \gamma w \ldots$$

annehmen, worin $u, v, w, \ldots$ Variable sind, so giebt es nach Voraussetzung ein ganzes Functional ω, so dass $\mu = \delta\omega$ ist. Das Functional ω stellen wir als Quotienten zweier ganzer Functionen $\varphi : \varepsilon$ dar, von denen ε eine Einheit, und folglich φ eine Function mit ganzzahligen Coëfficienten ist, und erhalten so

(6) $$\varepsilon\mu = (\alpha u + \beta v + \gamma w + \cdots)\,\varphi.$$

Ordnet man beide Seiten dieser Gleichung nach den darin vorkommenden Variablen, so erhält man, wenn $\varepsilon_1, \varepsilon_2, \ldots$ die Coëfficienten in ε sind, ein System von Gleichungen von folgender Form:

(7) $$\begin{aligned} \varepsilon_1\mu &= \alpha\xi_1 + \beta\eta_1 + \gamma\zeta_1 + \cdots \\ \varepsilon_2\mu &= \alpha\xi_2 + \beta\eta_2 + \gamma\zeta_2 + \cdots \\ &\cdots\cdots\cdots\cdots, \end{aligned}$$

worin die $\xi_i, \eta_i, \zeta_i, \ldots$ Zahlen in $\mathfrak{o}$ sind. Nun haben aber die Zahlen $\varepsilon_1, \varepsilon_2, \ldots$ als Coëfficienten einer Einheit, keinen gemein-

samen Theiler, und folglich kann man nach 3. die Zahlen $\tau_1, \tau_2, \ldots$ in $\mathfrak{o}$ so bestimmen, dass

(8) $$\varepsilon_1 \tau_1 + \varepsilon_2 \tau_2 + \cdots = 1$$

wird. Aus (7) folgt aber, wenn man mit $\tau_1, \tau_2, \ldots$ multiplicirt und addirt, und dann

$$\xi = \tau_1 \xi_1 + \tau_2 \xi_2 + \cdots, \quad \eta = \tau_1 \eta_1 + \tau_2 \eta_2 + \cdots$$

setzt, mittelst (8) die zu beweisende Gleichung (5).

§. 150.

Der Fermat'sche Satz.

Aus der Theorie der Congruenzen lassen sich Folgerungen ziehen, die den aus dem Fermat'schen Lehrsatze abgeleiteten Sätzen der rationalen Zahlentheorie genau entsprechen, von denen hier die wichtigsten, späterer Anwendung wegen, besprochen werden müssen.

Wir wollen unter π ein Primfunctional f^{ten} Grades verstehen, also, wenn p die durch π theilbare natürliche Primzahl ist,

(1) $$N_a(\pi) = p^f$$

setzen (§. 140). Ist dann α irgend eine durch π nicht theilbare Zahl in $\mathfrak{o}$, so wird, wie wir schon im vorigen Paragraphen gesehen haben, das Product $\alpha \xi$ zugleich mit der Zahl ξ ein volles Restsystem nach dem Modul π durchlaufen. Lassen wir die durch π theilbare Zahl weg, so bleiben $N_a(\pi) - 1$ Zahlen übrig, und wenn wir das Product bilden, so folgt

(2) $$\alpha^{p^f - 1} \Pi(\xi) \equiv \Pi(\xi) \pmod{\pi},$$

wenn $\Pi(\xi)$ das Product aller Zahlen eines vollen Restsystems (mit Ausschluss der Null) bedeutet, und daher durch π nicht theilbar ist. Demnach folgt aus (2)

(3) $$\alpha^{p^f - 1} \equiv 1 \pmod{\pi},$$

oder, wenn man mit α multiplicirt,

(4) $$\alpha^{p^f} \equiv \alpha \pmod{\pi},$$

und in der letzten Form gilt der Satz auch noch, wenn α durch π theilbar ist.

Die Formeln (3), (4), die genau dem Fermat'schen Lehrsatze entsprechen (Bd. I, §. 136), sollen auch hier als Fermat'scher Lehrsatz bezeichnet werden.

Wir sprechen ihn so aus:

1. Ist π ein Primtheiler der natürlichen Primzahl p, so ist für jede ganze Zahl ω im Körper Ω
$$\omega^{N_a(\pi)} \equiv \omega \pmod{\pi}.$$

Hieran knüpfen sich nun wichtige Folgerungen:

2. Bezeichnet $f(t)$ eine ganze Function m^{ten} Grades, deren Coëfficienten ganze Zahlen in Ω sind, und π ein Primfunctional, so hat die Congruenz
(5) $$f(t) \equiv 0 \pmod{\pi}$$
höchstens m Wurzeln, d. h. es giebt höchstens m incongruente ganze Zahlen in Ω, die, für t gesetzt, die Congruenz befriedigen.

Bedeutet nämlich α irgend eine Zahl in $\mathfrak{o}$, so können wir
(6) $$f(t) = (t-\alpha) f_1(t) + f(\alpha)$$
setzen, worin $f_1(t)$ eine ebensolche Function wie $f(t)$ ist, aber nur vom $(m-1)^{\text{ten}}$ Grade. Ist aber $f(\alpha) \equiv 0 \pmod{\pi}$, so muss jede Wurzel von (5) der Congruenz
$$(t-\alpha) f_1(t) \equiv 0 \pmod{\pi}$$
genügen. Sie muss also entweder mit α congruent oder eine Wurzel der Congruenz $(m-1)^{\text{ten}}$ Grades
$$f_1(t) \equiv 0 \pmod{\pi}$$
sein. Setzen wir unseren Satz als bewiesen voraus für Congruenzen $(m-1)^{\text{ten}}$ Grades, so gilt er demnach auch für Congruenzen m^{ten} Grades; und da er für Congruenzen ersten Grades gilt, so ist er allgemein richtig.

Jede durch π nicht theilbare Zahl in $\mathfrak{o}$ genügt, wie wir gesehen haben, der Congruenz
(7) $$\omega^{p^f-1} \equiv 1 \pmod{\pi}.$$

Ist nun a die kleinste natürliche Zahl, für die die Congruenz
(8) $$\omega^a \equiv 1 \pmod{\pi}$$
befriedigt ist, so lässt sich durch das schon oft angewandte Schlussverfahren zeigen, dass jeder andere Exponent l, für den $\omega^l \equiv 1$ ist, ein Vielfaches von a sein muss. Denn wäre l nicht durch a theilbar, so wäre auch, wenn a' der Rest der Division von a durch l ist, $\omega^{a'} \equiv 1$, was nach der Voraussetzung über a nicht möglich ist. Also ist a ein Theiler von $p^f - 1$, und wir nennen ω eine zum Exponenten a gehörige Zahl.

Gehört ω zum Exponenten a, so sind die Potenzen

(9) $$1,\ \omega,\ \omega^2,\ \ldots,\ \omega^{a-1}$$

alle incongruent und bilden also, da sie alle der Congruenz (8) genügen (nach 2.), die Gesammtheit der Wurzeln dieser Congruenz. Unter den Zahlen (9) müssen daher alle anderen zum Exponenten a gehörigen Zahlen ω gesucht werden. Es wird aber ω^l nur dann zum Exponenten a gehören, wenn l relativ prim zu a ist, und es folgt:

Wenn es überhaupt Zahlen ω giebt, die zum Exponenten a gehören, so ist ihre Anzahl so gross, wie die Anzahl der relativen Primzahlen zu a in der Reihe der Zahlen $0, 1, 2, \ldots, a-1$. Diese Zahl bezeichnen wir, wie schon früher (Bd. I, §. 132), mit $\varphi(a)$. Dass aber zu jedem Theiler a von $p^f - 1$ immer wenigstens eine Zahl ω und folglich $\varphi(a)$ Zahlen gehören, kann man ganz so beweisen, wie der entsprechende Satz der rationalen Zahlentheorie im §. 136 des ersten Bandes bewiesen ist.

Die Zahlen ω, die zu dem Exponenten $p^f - 1$ gehören, deren es hiernach immer $\varphi(p^f - 1)$ giebt, heissen **primitive Wurzeln** von π. Ist γ eine solche primitive Wurzel, so bilden die Potenzen

$$1,\ \gamma,\ \gamma^2,\ \ldots,\ \gamma^{p^f-2}$$

ein volles Restsystem nach dem Modul π mit Ausschluss der durch π theilbaren Zahl.

Nach dem Fermat'schen Lehrsatze für rationale Zahlen ist $t^{p-1} - 1$ für $t = 1, 2, \ldots, p-1$ durch p, und folglich auch durch π theilbar. Die Congruenz

(10) $$t^{p-1} \equiv 1 \pmod{\pi}$$

hat daher die Wurzeln

$$1,\ 2,\ \ldots,\ p-1,$$

und diese sind, da nach §. 140, 3. eine rationale Zahl nur dann durch π theilbar ist, wenn sie durch p theilbar ist, unter einander incongruent. Nach dem Satze 2. hat also die Congruenz (10) keine anderen Wurzeln als diese.

Multipliciren wir die Congruenz (10) noch mit t, so folgt, dass die Congruenz p^{ten} Grades

$$t^p - t \equiv 0 \pmod{\pi}$$

die p Wurzeln

$$0,\ 1,\ 2,\ \ldots,\ p-1,$$

ıd keine anderen hat. Darin liegt der Beweis des folgenden ,tzes:

3. Eine Zahl ω in $\mathfrak{o}$ ist dann und nur dann nach dem Modul π mit einer rationalen Zahl congruent, wenn sie der Bedingung

$$\omega^p \equiv \omega \pmod{\pi}$$

genügt.

Beachtet man noch, dass die Polynomialcoëfficienten in der ᵐ Potenz eines Polynoms alle durch p theilbar sind, mit Ausıhme derer, die zu den p^{ten} Potenzen der einzelnen Glieder ıs Polynoms gehören, so ergiebt sich noch folgender Satz, der ;h auf ganze Functionen in Ω von beliebigen Veränderlichen $y, \ldots$ bezieht:

4. Ist $\psi(x, y, \ldots)$ eine ganze Function der Variablen $x, y, \ldots$ mit ganzzahligen Coëfficienten aus Ω, so ist das Bestehen der Congruenz

$$[\psi(x, y, \ldots)]^p \equiv \psi(x^p, y^p, \ldots) \pmod{\pi}$$

die nothwendige und hinreichende Bedingung dafür, dass alle Coëfficienten von ψ mit ganzen rationalen Zahlen nach dem Modul π congruent sind.

§. 151.

Die Dedekind'schen Ideale.

Dedekind gründet in den schon oben erwähnten Arbeiten e Theorie der algebraischen Zahlen auf den Begriff des Ideals.

Wir wollen jetzt nachweisen, dass die Theorie der Ideale ı Wesen übereinstimmt mit der Theorie der Functionale, in-ɔm wir zeigen, wie der Uebergang von der einen zur anderen ɔwirkt werden kann.

Das System aller ganzen Zahlen eines algebraischen Zahl-ırpers Ω soll, wie oben, mit $\mathfrak{o}$ bezeichnet werden[1]). Ein in $\mathfrak{o}$ ıthaltenes Zahlensystem $\mathfrak{a}$ wird ein Ideal genannt, wenn es ɔn beiden Forderungen genügt:

---

[1]) Vgl. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie im 167 der dritten, §. 177 der vierten Auflage.

I. Summe und Differenz irgend zweier Zahlen in $\mathfrak{a}$ geben immer wieder Zahlen in $\mathfrak{a}$.

II. Das Product irgend einer Zahl in $\mathfrak{a}$ und einer Zahl in $\mathfrak{o}$ gehört dem System $\mathfrak{a}$ an.

Dieser Forderung würde das aus der einzigen Zahl Null bestehende System genügen, was aber der Einfachheit halber nicht als ein Ideal bezeichnet wird.

Das System $\mathfrak{o}$ dagegen ist ein eigentliches Ideal. Ebenso ist das System aller durch eine bestimmte Zahl μ in $\mathfrak{o}$ theilbaren Zahlen $\mathfrak{o}\mu$ ein Ideal, und ein solches wird ein **Hauptideal** genannt.

Unter dem Producte $\mathfrak{a}\mathfrak{b}$ zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$ versteht man den Inbegriff aller Zahlen, die man erhält, wenn man irgend eine Zahl α aus $\mathfrak{a}$ mit einer Zahl β aus $\mathfrak{b}$ multiplicirt und eine beliebige Anzahl solcher Zahlenproducte addirt, also den Inbegriff aller Zahlen von der Form $\Sigma\alpha\beta$. Dass dieses Product $\mathfrak{a}\mathfrak{b}$ wieder ein Ideal ist, leuchtet unmittelbar ein. Nach dieser Definition ist z. B. $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$, und das Ideal $\mathfrak{o}$ spielt bei dieser Multiplication die Rolle der Einheit.

Man kann nun die Ideale und Functionale in der Weise auf einander beziehen, dass dabei folgende Gesetze obwalten:

1. Jedem ganzen Functional entspricht ein bestimmtes Ideal, und associirten Functionalen entspricht dasselbe Ideal.
2. Jedem Ideal entsprechen unendlich viele, aber nur associirte ganze Functionale.
3. Dem Producte zweier oder mehrerer ganzer Functionale entsprechen die Producte der den Factoren entsprechenden Ideale.
4. Einer ganzen Zahl entspricht ein Hauptideal.
5. Den Einheiten entspricht das Ideal $\mathfrak{o}$.

Um dieses Entsprechen zu definiren, ordnen wir zunächst dem Systeme aller Einheiten das Ideal $\mathfrak{o}$ zu. Ist dann ferner φ irgend ein ganzes Functional, was keine Einheit ist, so genügt der Inbegriff aller durch φ theilbaren ganzen Zahlen α des Körpers Ω nach §. 138 den Forderungen I, II, und ist also ein Ideal, das wir mit $\mathfrak{a}$ bezeichnen[1]) und dem Functional φ zu-

[1]) Zur Bezeichnung der Ideale gebrauchen wir mit Dedekind die kleinen deutschen Buchstaben.

ordnen. Dasselbe Ideal $\mathfrak{a}$ ist dann auch sämmtlichen mit φ associirten Functionalen zugeordnet. Diese Zuordnung hat die Eigenschaften 1., 4., 5.

Sind φ und φ_1 zwei nicht associirte Functionale, so ist gewiss eines von ihnen, etwa φ, nicht durch das andere φ_1 theilbar, und folglich giebt es (nach §. 143, 3.) ganze Zahlen, die durch φ, aber nicht durch φ_1 theilbar sind. Folglich sind nicht associirten Functionalen immer verschiedene Ideale $\mathfrak{a}$, $\mathfrak{a}_1$ zugeordnet.

Es ist aber nun auch zu zeigen, dass auf diese Weise alle Ideale des Körpers Ω erhalten werden können, mit anderen Worten, dass jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ aus der Gesammtheit der durch einen gewissen Functionalfactor theilbaren Zahlen besteht.

Wir gehen also jetzt von irgend einem Ideal $\mathfrak{a}$ aus und wählen eine beliebige endliche Menge von Zahlen daraus, $\alpha_1, \alpha_2, \ldots, \alpha_r$, deren grösster gemeinschaftlicher Theiler δ_r sein mag. Dieses Functional δ_r hat eine endliche Anzahl von Primfactoren.

Giebt es nun eine Zahl α_{r+1} in $\mathfrak{a}$, die nicht durch δ_r theilbar ist, so hat der grösste gemeinschaftliche Theiler δ_{r+1} von δ_r und α_{r+1} weniger Primfactoren als δ_r. Wenn wir mit dieser Schlussweise fortfahren, so kommen wir zu dem Ergebniss, dass sich aus $\mathfrak{a}$ eine endliche Zahl von Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_m$ so auswählen lässt, dass der grösste gemeinschaftliche Theiler δ dieser Zahlen in allen Zahlen von $\mathfrak{a}$ aufgeht.

Andererseits gehört jede durch δ theilbare Zahl in $\mathfrak{o}$ zu $\mathfrak{a}$. Denn nach §. 149, 4. kann jede durch δ theilbare Zahl α in die Form gesetzt werden

$$\alpha = \alpha_1 \xi_1 + \alpha_2 \xi_2 + \cdots + \alpha_m \xi_m,$$

worin $\xi_1, \xi_2, \ldots, \xi_m$ Zahlen in $\mathfrak{o}$ sind, und folglich gehört nach I. und II. α zum Ideal $\mathfrak{a}$.

Es ergiebt sich hieraus, dass, wenn δ eine Einheit ist, das Ideal $\mathfrak{a}$ mit $\mathfrak{o}$ identisch ist. Jedes Ideal $\mathfrak{a}$ ist also dadurch charakterisirt, dass alle seine Zahlen einen gewissen grössten gemeinschaftlichen Theiler haben.

Es bleibt noch zu zeigen, dass, wenn die Functionale φ, ψ den beiden Idealen $\mathfrak{a}, \mathfrak{b}$ entsprechen, das Product $\varphi\psi$ dem Ideal $\mathfrak{a}\mathfrak{b}$ entspricht.

Da alle Zahlen aus $\mathfrak{a}\mathfrak{b}$ von der Form $\Sigma \alpha \beta$ sind, so ist zunächst klar, dass alle diese Zahlen durch $\varphi \psi$ theilbar sind.

Wenn wir aber nach §. 143, 4. das Functional φ als grössten gemeinschaftlichen Theiler zweier Zahlen α_1, α_2 darstellen, so gehören diese Zahlen, als durch φ theilbar, dem Ideal $\mathfrak{a}$ an, und wir können, da es auf einen Einheitsfactor bei φ nicht ankommt,

$$\varphi = \alpha_1 x_1 + \alpha_2 x_2$$

setzen, wenn x_1, x_2 Variable sind. Ebenso können wir, wenn β_1, β_2 zwei Zahlen aus $\mathfrak{b}$ und y_1, y_2 Variable bedeuten,

$$\psi = \beta_1 y_1 + \beta_2 y_2$$

setzen, und daraus ergiebt sich

$$\varphi \psi = \alpha_1 \beta_1 x_1 y_1 + \alpha_1 \beta_2 x_1 y_2 + \alpha_2 \beta_1 x_2 y_1 + \alpha_2 \beta_2 x_2 y_2.$$

Es ist also $\varphi \psi$ nach §. 143, 2. der grösste gemeinschaftliche Theiler der vier Zahlen $\alpha_1 \beta_1, \alpha_1 \beta_2, \alpha_2 \beta_1, \alpha_2 \beta_2$, die dem Ideal $\mathfrak{a}\mathfrak{b}$ angehören, und folglich ist $\varphi \psi$ der grösste gemeinschaftliche Theiler aller Zahlen des Ideals $\mathfrak{a}\mathfrak{b}$.

Damit ist die gegenseitige Zuordnung der Functionale und Ideale den Forderungen 1. bis 5. gemäss bewerkstelligt.

Den Primfunctionalen entsprechen bei dieser Zuordnung Primideale, und die Zerlegung der Ideale in Primfactoren und überhaupt die Gesetze der Theilbarkeit der Ideale ergeben sich in völliger Uebereinstimmung mit den entsprechenden Sätzen aus der Theorie der Functionale.

Bei dieser völligen Uebereinstimmung kann es zu keiner Unzuträglichkeit führen, wenn wir das ganze System aller unter einander associirten Functionale zu einem Gemeinbegriffe zusammenfassen und dafür den Namen Ideal brauchen.

Das System aller mit einer ganzen Zahl associirten Functionale ist dann ein Hauptideal.

Wenn irgend eine Zahl oder ein Functional durch die Functionale eines Ideals theilbar ist, so nennen wir es durch das Ideal theilbar, und wenn ein Functional φ in Factoren zerlegt ist, denen die Ideale $\mathfrak{a}, \mathfrak{b}, \ldots$ entsprechen, so setzen wir auch, indem die Einheitsfactoren in der Bezeichnung weggelassen werden:

$$(1) \qquad \varphi = \mathfrak{a}\,\mathfrak{b} \ldots$$

Eine Basis des Functionals ist zugleich eine Basis des Ideals, und die absolute Norm des repräsentirenden Functionals stimmt

mit der Zahl überein, die bei Dedekind die Norm des Ideals heisst. Sie soll also auch hier so genannt werden, und wir setzen demnach, wenn das Functional φ zu dem Ideal $\mathfrak{a}$ gehört,

$$(2) \qquad N_{\mathfrak{a}}(\varphi) = N(\mathfrak{a}).$$

Die Norm eines Ideals ist also immer eine natürliche Zahl.

Ist $\mathfrak{p}$ ein Primideal und p die durch $\mathfrak{p}$ theilbare natürliche Primzahl, so ist

$$(3) \qquad N(\mathfrak{p}) = p^f,$$

und f heisst der Grad des Primideals $\mathfrak{p}$.

In den Congruenzen (§. 149, 150) können nach diesen Festsetzungen statt der Functionale auch die entsprechenden Ideale als Moduln angesehen werden.

Es sei schliesslich noch ein Wort über die Kummer'sche Schöpfung der idealen Zahlen beigefügt[1]).

Sind α, β irgend zwei Zahlen aus $\mathfrak{o}$, die den grössten gemeinschaftlichen Theiler χ haben, und ist $\beta = \chi\,\varphi$, so wird die Congruenz

$$(4) \qquad \alpha\,\omega \equiv 0 \pmod{\beta}$$

nur für solche Zahlen ω aus $\mathfrak{o}$ befriedigt sein, die durch φ theilbar sind. Das Functional φ wird aber im Allgemeinen keiner Zahl associirt sein. Statt nun die Functionale zu benutzen, kann man sich ein neues Begriffssystem schaffen, in dem man die sämmtlichen Zahlen von $\mathfrak{o}$ zu Paaren zusammenfasst (α, β), und kann diese Paare „ideale Zahlen" in $\mathfrak{o}$ nennen; genau in derselben Weise, wie man durch Paarung der ganzen rationalen Zahlen die Brüche, oder der reellen Zahlen die complexen Zahlen gebildet hat.

Man nennt dann die Zahl ω durch die ideale Zahl (α, β) theilbar, wenn sie der Congruenz (1) genügt. Dies ist der Standpunkt der Kummer'schen Theorie. Damit aber diese Definition der Theilbarkeit fruchtbar sei, muss noch festgestellt werden, unter welchen Voraussetzungen man zwei ideale Zahlen mit verschiedenen Elementen, (α, β), (α', β'), als gleich zu betrachten hat, wie sich die wirklichen Zahlen in $\mathfrak{o}$ unter die idealen Zahlen einordnen, endlich was man unter dem Product zweier idealen Zahlen zu verstehen hat, damit eine durch eine ideale Zahl

---

1) Vgl. Dirichlet-Dedekind, Zahlentheorie, §. 176.

theilbare Zahl sich als Product von idealen Zahlen darstellen lasse. Alle diese Fragen werden beantwortet durch die Vermittelung der Functionaltheorie (oder der Idealtheorie), wenn man der idealen Zahl (α, β) das Functional φ zuordnet, und können wohl kaum auf einfachere Weise entschieden werden. Die Einführung des Systemes der idealen Zahlen bietet dann auch keine wesentlichen Vortheile mehr, und man kann ebenso gut die Functionale selbst, oder die Ideale als Elemente der neu einzuführenden Mannigfaltigkeit betrachten.

§. 152.

Aequivalenz.

Wir nennen jetzt zwei Functionale, die sich nur durch einen Einheitsfactor unterscheiden, auch wenn sie gebrochen sind, associirt, und stellen folgende Definition auf:

1. Zwei ganze oder gebrochene Functionale φ, ψ im Körper Ω heissen äquivalent, wenn ihr Quotient $\varphi : \psi$ mit einer Zahl associirt ist.

Es heissen also die beiden Functionale φ und ψ äquivalent, wenn eine Einheit ε und eine Zahl α in Ω existiren, so dass

$$\frac{\varphi}{\psi} = \alpha \varepsilon \tag{1}$$

ist. Ist φ äquivalent mit ψ und mit ψ_1, so folgt aus (1)

$$\frac{\varphi}{\psi} = \alpha \varepsilon, \quad \frac{\varphi}{\psi_1} = \alpha_1 \varepsilon_1,$$

folglich

$$\frac{\psi}{\psi_1} = \frac{\alpha_1}{\alpha} \frac{\varepsilon_1}{\varepsilon},$$

und da $\alpha_1 : \alpha$ eine Zahl, $\varepsilon_1 : \varepsilon$ eine Einheit ist, so folgt der erste Satz:

2. Zwei Functionale, die mit einem dritten äquivalent sind, sind auch unter einander äquivalent.

Theilt man hiernach alle Functionale des Körpers Ω in Classen ein, indem man zwei Functionale in dieselbe oder in verschiedene Classen wirft, je nachdem sie äquivalent sind oder nicht, so ergiebt sich, dass zwei dieser Classen, die ein einziges

gemeinsames Element enthalten, vollständig identisch sein müssen, und die Classeneintheilung ist also durchaus eindeutig. Jede Classe ist durch ein beliebiges in ihr enthaltenes Functional, einen Repräsentanten, völlig bestimmt.

3. Zwei mit einander associirte Functionale sind auch äquivalent und kommen daher in derselben Classe vor.

Denn wenn φ und ψ associirt sind, so ist ihr Quotient $\varphi : \psi$ eine Einheit, und φ und ψ sind also auch äquivalent.

Eine Classe enthält aber nicht bloss die einzelnen Functionale φ, sondern alle durch diese Functionale bestimmten Ideale, und wir nennen diese Classen daher, wenn eine genauere Bezeichnung nöthig ist, Functionalclassen oder, häufiger noch, dem üblichen Sprachgebrauche gemäss, Idealclassen.

4. Die Gesammtheit aller ganzen und gebrochenen Zahlen des Körpers Ω, verbunden mit den sämmtlichen Einheiten und den Producten von Zahlen mit Einheiten, bilden unter sich eine Classe, die die Hauptclasse genannt wird.

Als Repräsentanten der Hauptclasse kann man z. B. die Zahl 1 betrachten. Die Hauptclasse, als Idealclasse aufgefasst, enthält das Ideal $\mathfrak{o}$ und wird daher in der Folge durch den Buchstaben O bezeichnet.

5. In jeder Idealclasse giebt es ganze Functionale.

Denn nach der Definition ist, wenn φ irgend ein Functional und α eine Zahl ist, φ mit $\alpha\varphi$ äquivalent. Wir können aber nach §. 137, 5. die Zahl α, sogar rational, so bestimmen, dass $\alpha\varphi$ ein ganzes Functional wird.

6. Aus jeder Idealclasse C können wir einen Repräsentanten φ auswählen, der nicht nur selbst ein ganzes Functional ist, sondern auch zu einem beliebig gegebenen ganzen Functional ω relativ prim ist.

Nehmen wir, um diesen Satz zu beweisen, zunächst nach 5. einen beliebigen ganzen Repräsentanten φ der Classe C und eine durch φ theilbare ganze Zahl α, so ist

$$\varphi\chi = \alpha, \tag{2}$$

und χ ein ganzes Functional. Nun wählen wir (nach §. 143, 3.) eine durch χ theilbare Zahl β so, dass $\beta : \chi$ relativ prim zu ω wird, und setzen

(3) $$\psi\chi = \beta.$$

Da jetzt $\varphi : \psi$ eine Zahl ist, so ist ψ mit φ äquivalent, und ψ ist ein zu ω theilerfremder Repräsentant der Classe C[1]).

§. 153.

Die Classenzahl des Körpers Ω.

Wir kommen nun zum Beweise des wichtigen Satzes:

1. Die Anzahl der Idealclassen eines Körpers Ω ist endlich.

Dieser Satz ist gleichbedeutend mit dem folgenden:

2. In jeder Classe giebt es ganze Functionale, deren absolute Norm eine bestimmte endliche, nur von der Natur des Körpers Ω abhängige Zahl nicht übersteigt.

Denn weil jedes ganze Functional ein Factor seiner absoluten Norm ist, und jede ganze Zahl nur eine endliche Anzahl von nichtassociirten Factoren hat, so giebt es, von den associirten abgesehen, nur eine endliche Zahl von ganzen Functionalen, die eine gegebene Zahl zur absoluten Norm haben. Wenn nun bewiesen werden kann, dass in jeder Classe ein ganzes Functional vorkommt, dessen absolute Norm unter einer endlichen Zahl

---

[1]) Wir wollen hier im Vorübergehen auf eine Analogie der Aequivalenz der Ideale hinweisen. Die ganze Theorie der algebraischen Zahlen lässt sich mit den nothwendigen Modificationen übertragen auf die Theorie der algebraischen Functionen, die wieder ihren geometrischen Ausdruck in der Theorie der algebraischen Curven findet. Den Idealen entsprechen dann Punktsysteme auf einer festen Grundcurve und den Hauptidealen volle Schnittpunktsysteme der Grundcurve mit einer anderen algebraischen Curve. Wenn sich zwei Punktsysteme zu einem vollen Schnittpunktsystem ergänzen, was in der obigen Formel $\varphi\chi = \alpha$ seinen Ausdruck finden würde, so wird von den beiden Punktsystemen φ, χ jedes der Rest des anderen genannt. Zwei Punktsysteme, die, wie φ, ψ, denselben Rest haben, werden in der Geometrie corresidual genannt. Dieser Begriff entspricht also der Aequivalenz. (Vergl. Brill u. Nöther, Mathem. Annalen, Bd. 7. Salmon, „higher plane Curves“, deutsch von Fiedler.)

liegt, so ist die Endlichkeit der Anzahl der Classen nachgewiesen.

Lassen wir, wie bisher, $\omega_1, \omega_2, \ldots, \omega_n$ eine Minimalbasis von Ω bedeuten, so werden alle ganzen Zahlen des Körpers aus

$$(1) \qquad \omega = \omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n$$

erhalten, wenn wir den $x_1, x_2, \ldots, x_n$ ganze rationale Zahlwerthe ertheilen. Wenn wir eine positive ganze Zahl k annehmen und festsetzen, dass keine der Zahlen x_i aus dem Intervall $\pm k$ heraustreten soll, so wird der absolute Werth von ω nicht über der Grenze

$$(|\omega_1| + |\omega_2| + \cdots + |\omega_n|)\, k = r k$$

liegen, wenn unter $|\omega_1|, |\omega_2|, \ldots$ die absoluten Werthe (Einleitung, Bd. I, S. 18) der (reellen oder complexen) Grössen ω_i verstanden sind, und r die Summe $|\omega_1| + |\omega_2| + \cdots$ bedeutet. Bilden wir den Ausdruck (1) für die n conjugirten Körper, und nehmen das Product, so erhalten wir, wenn wir mit R eine positive reelle Zahl bezeichnen, die über dem Product der n Werthe r liegt,

$$(2) \qquad N_a(\omega) < R\, k^n.$$

Diese Zahl R ist nur von der Natur des Körpers Ω, nicht aber von k abhängig.

Jetzt sei μ irgend ein ganzes Functional in Ω, und $N_a(\mu)$ seine absolute Norm. Wenn wir die ganze Zahl k so bestimmen, dass

$$(3) \qquad k^n \leqq N_a(\mu) < (k+1)^n,$$

und wenn wir ferner in (1) den Zahlen x_i die Werthe $0, 1, 2, \ldots, k$ ertheilen, so ist die Anzahl der verschiedenen Werthe, die aus (1) hervorgehen, $(k+1)^n$, also grösser als $N_a(\mu)$. Nach §. 148, 3. ist aber die Zahl der nach dem Modul μ incongruenten Zahlen gleich $N_a(\mu)$, und folglich müssen unter den so bestimmten Zahlen ω mindestens zwei verschiedene nach dem Modul μ congruente Zahlen vorkommen. Ist also $\omega' \equiv \omega''$ (mod μ), so wird die Differenz

$$(4) \qquad \alpha = \omega' - \omega'' = (x'_1 - x''_1)\, \omega_1 + \cdots + (x'_n - x''_n)\, \omega_n$$

durch μ theilbar sein, und zugleich sind die ganzen Zahlen

$$x'_1 - x''_1 = a_1, \ldots, x'_n - x''_n = a_n$$

absolut genommen nicht grösser als k. Es giebt eine durch μ theilbare von Null verschiedene Zahl:

$$(5) \qquad \alpha = a_1 \omega_1 + a_2 \omega_2 + \cdots + a_n \omega_n,$$

in der die ganzzahligen Coëfficienten $a_1, a_2 \ldots a_n$ die Grenzen $\pm k$ nicht überschreiten, und folglich ist nach (2) und (3)

$$(6) \qquad N_a(\alpha) < R k^n < R\, N_a(\mu).$$

Da nun α durch μ theilbar ist, so setzen wir

$$(7) \qquad \alpha = \mu \varphi,\ N_a(\alpha) = N_a(\mu)\, N_a(\varphi),$$

und erhalten aus (6)

$$(8) \qquad N_a(\varphi) < R.$$

Wenn nun ψ ein Repräsentant einer beliebig gegebenen Classe C ist, so wählen wir μ so, dass

$$\beta = \mu \psi$$

eine Zahl ist, und wenn dann nach (7)

$$\alpha = \mu \varphi$$

ist, so ist

$$\frac{\varphi}{\psi} = \frac{\alpha}{\beta},$$

also φ und ψ äquivalent. φ ist also gleichfalls ein Repräsentant der Classe C, und dieser genügt der Bedingung (8). Es kommt also, wie bewiesen werden sollte, in jeder Classe ein Functional vor, dessen absolute Norm unter R liegt.

Die Anzahl der Idealclassen, die wir mit h bezeichnen wollen, ist hiernach eine dem Körper Ω eigenthümliche natürliche Zahl, die die Classenzahl genannt wird.

In dem einfachsten Falle, wo die Classenzahl gleich 1 ist, ist jedes Functional mit einer Zahl associirt, d. h. es kann jedes (ganze oder gebrochene) Functional durch Absonderung eines Zahlenfactors in eine Einheit verwandelt werden. In diesem Falle lässt sich jede ganze Zahl des Körpers Ω in Primzahlfactoren zerlegen, und diese Körper haben eine Theorie, die im Wesentlichen mit der rationalen Zahlentheorie übereinstimmt. Für solche Körper ist die Einführung der Functionale und Ideale nicht nothwendig.

Hierher gehören neben dem Körper der rationalen Zahlen unter anderen der Körper der Gauss'schen imaginären Zahlen und der aus dritten Einheitswurzeln gebildeten Zahlen (Bd. I, §. 173, 174).

§. 154.

Die Gruppe der Idealclassen.

Die Idealclassen können auf Grund des folgenden Satzes componirt werden:

1. Sind φ, ψ, φ_1, ψ_1 Functionale und φ äquivalent mit φ_1, ψ äquivalent mit ψ_1, so ist auch $\varphi\psi$ äquivalent mit $\varphi_1\psi_1$.

Die Richtigkeit hiervon ergiebt sich unmittelbar aus der Definition. Denn wenn $\varphi : \varphi_1$ und $\psi : \psi_1$ mit Zahlen associirt sind, so ist auch $\varphi\psi : \varphi_1\psi_1$ mit einer Zahl associirt.

Ebenso ergiebt sich auch der umgekehrte Satz:

2. Ist φ äquivalent mit φ_1 und $\varphi\psi$ äquivalent mit $\varphi_1\psi_1$, so ist auch ψ äquivalent mit ψ_1.

Betrachten wir also zwei Idealclassen A, B, die auch identisch sein können, und bilden das Product $\varphi\psi$ irgend eines Functionals φ aus A und eines Functionals ψ aus B, so ist die Classe C, in der das Product $\varphi\psi$ vorkommt, unabhängig von der Wahl von φ und ψ, und die Classe C ist durch die beiden Classen A, B völlig bestimmt. Wir nennen C aus A und B componirt und schreiben symbolisch

$$C = AB = BA. \tag{1}$$

Die Classe C enthält alle Producte eines Elementes von A mit einem Element von B, kann aber auch noch andere Functionale enthalten.

Da diese Composition aus der wahren Multiplication abgeleitet ist, so gelten auch die Gesetze der Multiplication für diese Composition, nämlich das commutative und das associative Gesetz.

Es folgt ferner aus dem Satze 2., dass, wenn $AB = AB_1$ ist, auch $B = B_1$ sein muss, und folglich erzeugen die Idealclassen bei dieser Composition eine endliche Abel'sche Gruppe vom Grade h, auf die wir alle Sätze anwenden können, die wir im zweiten Abschnitt dieses Bandes über solche Gruppen kennen gelernt haben.

Die Einheit dieser Gruppe ist die schon im §. 152 definirte Hauptclasse O, die ja, wie wir gesehen haben, den Repräsen-

tanten 1 hat. Um entgegengesetzte Classen zu definiren, nehmen wir einen Repräsentanten φ einer Classe A und eine durch φ theilbare Zahl α. Ist dann $\alpha = \varphi \chi$, so ist χ ein Repräsentant der Classe A^{-1}, und es ist $A A^{-1} = O$.

Ist A eine beliebige Classe, und h die Classenzahl, so ist immer

$$A^h = O,$$

und wenn k die kleinste positive Zahl ist, die der Bedingung

$$A^k = O$$

genügt, so ist k ein Theiler von h. Daraus ergiebt sich der Satz:

3. Jedes Functional φ in Ω gehört zu einem bestimmten Exponenten k, der ein Theiler der Classenzahl h ist, so dass φ^k associirt ist mit einer Zahl in Ω.

Achtzehnter Abschnitt.

Discriminanten.

---

§. 155.

Minimum einer quadratischen Form.

Auf einem ganz neuen Weg hat Minkowski die Endlichkeit der Anzahl der Classen bewiesen [1]), der von eigenthümlichen, zahlreicher Anwendungen fähigen Betrachtungen ausgeht und dabei zu dem lange vergeblich gesuchten Beweis eines Satzes über die Körperdiscriminante führt. Wir wollen hier in der Kürze die Hauptmomente dieser Untersuchungen mittheilen.

Minkowski geht aus von der Betrachtung einer quadratischen Form von n Variablen

(1) $$f(x_1, x_2, \ldots, x_n) = \sum^{i,k} a_{i,k}\, x_i x_k$$

mit reellen Coëfficienten $a_{i,k}$, von der vorausgesetzt wird, dass sie sich in n und nicht weniger positive Quadrate linearer Functionen zerlegen lässt (einer positiven Form, Bd. I, §. 81 bis 83).

Es möge eine dieser Darstellungen sein

(2) $$f(x_1, x_2, \ldots, x_n) = \xi_1^2 + \xi_2^2 + \cdots + \xi_n^2,$$

worin

(3) $$\xi_i = \alpha_{1,i}\, x_1 + \alpha_{2,i}\, x_2 + \cdots + \alpha_{n,i}\, x_n$$

ein System linearer Functionen der x_i mit nicht verschwindender Determinante ist. Setzen wir

(4) $$A = \Sigma \pm \alpha_{1,1}\, \alpha_{2,2} \ldots \alpha_{n,n},$$

---

[1]) Ueber die positiven quadratischen Formen etc. Crelle, Bd. 107, 1891. Eingehender noch in dem Buche von Minkowski, „Geometrie der Zahlen“, Leipzig 1896.

so ist die Determinante D der quadratischen Form (1) (Bd. I, §. 59)

(5) $$D = \Sigma \pm a_{1,1}\, a_{2,2} \ldots a_{n,n} = A^2.$$

Die $\alpha_{i,k}$ sind dann gleichfalls reelle Zahlen, die auf unendlich viele Arten bestimmt werden können. Wir nehmen eine beliebige, aber weiterhin unveränderliche Transformation (2), (3) an.

Das Gleichungssystem (3) möge, nach den x aufgelöst, ergeben:

(6) $$x_i = \beta_{1,i}\, \xi_1 + \cdots + \beta_{n,i}\, \xi_n.$$

Wir wollen nun den Variablen x_i nur ganze rationale Zahlwerthe beilegen. Dann ist klar, dass die Function f nur verschwinden kann, wenn alle x_i verschwinden, und dass ihr Werth, wenn wir diesen Fall ausschliessen, nicht unter einen gewissen endlichen Grenzwerth M heruntersinken kann, den wir das Minimum der Form f nennen. Denn sinkt der Werth von f unter einen Werth α^2 herunter, so müssen nach (2) alle ξ_i dem absoluten Werthe nach unter α herunter sinken, und nach (6) würden für ein hinlänglich kleines α sämmtliche x_i unter 1 herabgedrückt werden und müssten dann, da es ganze Zahlen sind, alle gleich Null sein.

Es kommt vor Allem darauf an, nicht sowohl das Minimum genau zu bestimmen, als eine möglichst kleine obere Grenze dafür zu finden, über die es nicht hinausgehen kann.

Wir bedienen uns jetzt mit Minkowski einer Ausdrucksweise, die einer Geometrie im Raume von n Dimensionen entnommen ist, die ausserordentlich einfach zu dem gewünschten Resultat führt. Für die Fälle $n = 2$, $n = 3$ sind die dabei gebrauchten Ausdrücke vollständig anschaulich und allereinfachster Art. Wir empfehlen dem Leser, sich die nun auszuführenden Schritte an diesen beiden speciellen Fällen anschaulich klar zu machen. Bei grösseren Werthen von n geht freilich die eigentliche Anschauung verloren. Man hat dann diese Ausdrücke als kurze Bezeichnung gewisser analytischer Verhältnisse anzusehen, wobei noch die Analogie mit dem gewöhnlichen Raume die Auffassung erleichtert. Es hat nicht die geringste Schwierigkeit, alle diese Ausdrücke durch rein analytische Formeln zu ersetzen; es würde darunter aber sehr die Kürze des Ausdrucks und die Leichtigkeit der Auffassung leiden.

Wir bezeichnen also jetzt die Variablen $\xi_1, \ldots, \xi_n$ als Coor-

dinaten eines Punktes ξ in einem Raume von n Dimensionen R_ξ und nennen den Ausdruck

$$(7) \qquad \varrho = \sqrt{(\xi_1' - \xi_1'')^2 + (\xi_2' - \xi_2'')^2 + \cdots + (\xi_n' - \xi_n'')^2},$$

die Entfernung der beiden Punkte ξ', ξ''.

Wenn wir in (3) die Variablen x_i alle ganzzahligen Werthe durchlaufen lassen, so geben uns die zugehörigen Werthe der ξ_i ein Punktsystem im Raume R_ξ. Der Punkt, der den Werthen $x_i = 0$ entspricht, ist der Coordinaten-Anfangspunkt oder der Nullpunkt. Die Gesammtheit dieser Punkte bleibt ungeändert, wenn wir x_i durch $x_i + x_i^{(0)}$ ersetzen, wenn $x_1^{(0)}$, $x_2^{(0)}, \ldots, x_n^{(0)}$ ein festes System ganzer Zahlen bedeutet. Wir können diese Thatsache auch so ausdrücken, dass das Punktsystem der ξ_i mit sich selbst zur Deckung kommt, wenn es eine Parallelverschiebung erfährt, bei dem der Nullpunkt an den Ort eines beliebig gegebenen anderen Punktes des Systems gelangt; oder auch: Die Punkte des Systems sind zu jedem seiner Punkte in derselben Weise gelagert, wie zu jedem anderen.

Wir wollen dies System ein Punktgitter nennen und seine einzelnen Punkte die Gitterpunkte.

Nach (2) und (7) ist der Werth von f das Quadrat der Entfernung des Punktes ξ vom Nullpunkte und folglich ist $\sqrt{M}$ die kleinste Entfernung zweier Gitterpunkte, die in dem ganzen System vorkommt.

Ausser den Entfernungen in dem Raume R_n haben wir auch noch Volumina zu betrachten, d. h. die Werthe des n-fachen Integrals

$$(8) \qquad V_\xi = \int\int \ldots \int d\xi_1\, d\xi_2 \ldots d\xi_n,$$

worin die Variablen $\xi_1, \xi_2, \ldots, \xi_n$ irgend ein endliches Gebiet G_ξ erfüllen, was etwa durch eine oder mehrere Ungleichungen bestimmt ist. So ist das durch die Bedingung

$$(9) \qquad \xi_1^2 + \xi_2^2 + \cdots + \xi_n^2 \gtreqless 1 \text{ oder auch } \Sigma(\xi_i - \xi_i^0)^2 \gtreqless 1$$

bei beliebigen Werthen ξ_i^0 begrenzte Gebiet eine n-dimensionale Kugel vom Radius 1, deren Volumen wir mit K_n bezeichnen wollen. Aus jedem Gebiete G_ξ können wir ein ähnliches Gebiet $G_\xi^{(t)}$ ableiten, indem wir die Coordinaten alle im Verhältniss $t^{\frac{1}{n}} : 1$ vergrössern. Ist $V^{(t)}$ das Volumen des neuen Gebietes, so ist nach (8)

$$(10) \qquad V^{(t)} = t\,V.$$

Betrachten wir ausser dem Raume R_ξ noch einen zweiten Raum R_x, in dem die durch (3) oder (6) bestimmten Variablen x die Coordinaten sind, so entspricht jedem Punkte des einen Raumes ein und nur ein Punkt des anderen Raumes. Einem endliche Gebiete G_ξ entspricht ein endliches Gebiet G_x.

Um die Beziehung zwischen dem Volumen V_ξ und V_x zu ermitteln, müssen wir das Integral (8) nach den Regeln über die Umformung mehrfacher Integrale behandeln, wofür die allgemeine Formel gilt:

(11) $$\int\int\cdots\int d\xi_1\, d\xi_2 \ldots d\xi_n$$

$$=\int\int\cdots\int\sqrt{\left(\Sigma\pm\frac{d\xi_1}{dx_1}\frac{d\xi_2}{dx_2}\cdots\frac{d\xi_n}{dx_n}\right)^2}\, dx_1\, dx_2 \ldots dx_n$$ [1]).

Setzen wir darin für die Functionaldeterminante den Werth (4) oder (5) ein, so ergiebt sich

(12) $$V_\xi = \sqrt{D}\, V_x,$$

worin nun das Integral

(13) $$V_x = \int\int\cdots\int dx_1\, dx_2 \cdots dx_n$$

sich auf das Gebiet G_x bezieht.

Das Integral V_x können wir als Grenzwerth einer Summe von Elementen $\Delta x_1\, \Delta x_2 \ldots \Delta x_n$ auffassen, und wenn wir den Incrementen Δx_i allen die Grösse $1 : t^{\frac{1}{n}}$ geben, so wird jedes dieser Elemente den Werth $1 : t$ haben. Bedeutet Z_t die Anzahl dieser Elemente, so ist V_x der Grenzwerth, dem sich das Verhältniss $Z_t : t$ bei unendlich wachsendem t nähert, also

(14) $$V_x = \lim_{t=\infty}\frac{Z_t}{t}.$$

Nun ist die Anzahl der Elemente Z_t ebenso gross, wie die Anzahl der Punkte im Inneren von G_x, deren Coordinaten den Ausdruck

$$x_1 = h_1 t^{-\frac{1}{n}},\ x_2 = h_2 t^{-\frac{1}{n}},\ \ldots,\ x_n = h_n t^{-\frac{1}{n}}$$

mit ganzzahligen $h_1, h_2, \ldots, h_n$ haben, oder auch gleich der An-

[1]) Die allgemeine Formulirung dieser Umformung rührt von Jacobi her (De determinantibus functionalibus; Crelle, Bd. 22, 1891, gesammelte Werke, Bd. 3). Die Ableitung findet sich in den meisten ausführlicheren Lehrbüchern der Integralrechnung, z. B. Serret-Harnack, Bd. 2; Lipschitz, Lehrbuch der Analysis Bd. 2; auch Baltzer, Determinanten.

zahl der Punkte mit ganzzahligen Coordinaten, die in einem im Verhältniss $t^{\frac{1}{n}} : 1$ vergrösserten Gebiet $G_x^{(t)}$ liegen, und diese Zahl ist ebenso gross wie die Anzahl der Gitterpunkte, die in dem Gebiete $G_\xi^{(t)}$ liegen. Wir haben also folgenden Satz:

Ist G_ξ irgend ein endliches Gebiet im Raume R_ξ und $G_\xi^{(t)}$ das aus G_ξ durch Vergrösserung im Linearverhältniss $t^{\frac{1}{n}} : 1$ abgeleitete Gebiet; ist Z_t die Anzahl der im Inneren von $G_\xi^{(t)}$ liegenden Gitterpunkte, so ist das durch G_ξ bestimmte Volumen

$$(15) \qquad V_\xi = \sqrt{D} \lim_{t=\infty} \frac{Z_t}{t}.$$

Wir legen jetzt um jeden Gitterpunkt als Mittelpunkt eine n-dimensionale Kugel vom Radius $\frac{1}{2}\sqrt{M}$. Da $\sqrt{M}$ die kleinste Entfernung von irgend zwei Gitterpunkten ist, so können je zwei dieser Kugeln kein Gebiet gemein haben; sie können sich höchstens in einem Punkte berühren, und keine dieser Kugeln enthält ausser ihrem Mittelpunkte einen weiteren Gitterpunkt. Eine solche Kugel hat nach (10) das Volumen

$$K_n \left(\frac{\sqrt{M}}{2}\right)^n,$$

und das Gesammtvolumen aller der Kugeln, deren Mittelpunkt im Inneren von $G_\xi^{(t)}$ liegt, ist

$$V_1^{(t)} = Z_t K_n \left(\frac{\sqrt{M}}{2}\right)^n.$$

Dies Volumen $V_1^{(t)}$ ist aber offenbar kleiner als $V^{(t)}$, wenigstens wenn wir von den Kugeln, die zum Theil aus dem Gebiete $G^{(t)}$ herausragen, absehen, deren Gesammtvolumen, durch t dividirt, mit unendlich wachsendem t gegen Null convergirt, weil sein Gebiet nur einen Theil von $G^{(t)}$ erfüllt, und folglich ist auch V grösser als der Grenzwerth von $V_1^{(t)} : t$, also

$$V > \lim \frac{Z_t K_n}{t} \left(\frac{\sqrt{M}}{2}\right)^n,$$

und daraus nach (15)

$$(16) \qquad \sqrt{D} > K_n \left(\frac{\sqrt{M}}{2}\right)^n.$$

Da es nun leicht ist, das Volumen K_n zu bestimmen, so ist hierdurch die Aufgabe gelöst, und eine obere Grenze für M gefunden.

Wir wollen hier nicht den genauen Werth für K_n einsetzen, sondern einen einfacher auszudrückenden kleineren Werth, wodurch die Ungleichung (11) um so mehr richtig wird.

Nach der Definition ist

$$K_n = \int\int \cdots \int d\xi_1\, d\xi_2 \ldots d\xi_n, \tag{17}$$

mit der Begrenzung

$$\xi_1^2 + \xi_2^2 + \cdots + \xi_n^2 \leqq 1. \tag{18}$$

Die Grenzgleichung (18) ist sicher erfüllt, wenn wir die ξ_i auf die Intervalle

$$-\frac{1}{\sqrt{n}} < \xi_i < \frac{1}{\sqrt{n}} \tag{19}$$

beschränken, was geometrisch die Bedeutung hat, dass wir die Kugel durch den eingeschriebenen Würfel ersetzen. Demnach ist

$$K_n > \int_{-\frac{1}{\sqrt{n}}}^{\frac{1}{\sqrt{n}}} \int_{-\frac{1}{\sqrt{n}}}^{\frac{1}{\sqrt{n}}} \cdots \int_{-\frac{1}{\sqrt{n}}}^{\frac{1}{\sqrt{n}}} d\xi_1\, d\xi_2 \cdots d\xi_n,$$

und wenn diese Integration ausgeführt wird,

$$K_n > \left(\frac{2}{\sqrt{n}}\right)^n. \tag{20}$$

Die hierdurch bestimmte obere Grenze wird von K_n niemals erreicht, wenn wir von dem Falle $n = 1$ absehen.

Die Vergleichung von (20) mit (16) ergiebt einen sehr einfachen Ausdruck für den oberen Grenzwerth von M, nämlich

$$M < n \sqrt{D}, \tag{21}$$

und M ist (von dem Falle $n = 1$ abgesehen) wirklich kleiner, und nicht gleich dem Werthe $n \sqrt{D}$.

Dies zeigt sich klar, wenn man eine noch etwas engere Grenze für M aufsucht.

Die Bedingung (18) ist sicher dann erfüllt, wenn wir

$$-\alpha < \xi_n < \alpha, \quad \xi_1^2 + \xi_2^2 + \cdots + \xi_{n-1}^2 < 1 - \alpha^2 \tag{22}$$

setzen, wo α ein beliebiger positiver echter Bruch sein kann. (Die geometrische Bedeutung hiervon ist die, dass man die Kugel durch einen eingeschriebenen Cylinder von der Höhe 2α ersetzt). Es ist also

$$K_n > 2\alpha \int\int \cdots \int d\xi_1\, d\xi_2 \ldots d\xi_{n-1}$$
$$\xi_1^2 + \xi_2^2 + \cdots + \xi_{n-1}^2 < 1 - \alpha^2.$$

Wenn man in dem $(n-1)$fachen Integral ξ_i durch $\sqrt{1-\alpha^2}\,\xi_i$ ersetzt, so findet man dafür den Werth $\sqrt{(1-\alpha^2)}^{n-1}\,K_{n-1}$, und es findet sich also die Ungleichung

$$K_n > 2\alpha\,\sqrt{(1-\alpha^2)}^{n-1}\,K_{n-1}.$$

Nun wollen wir α so wählen, dass $2\alpha\,\sqrt{(1-\alpha^2)}^{n-1}$ so gross als möglich wird, und dafür findet man nach der gewöhnlichen Regel durch Nullsetzen des Differentialquotienten

$$\alpha = \frac{1}{\sqrt{n}}.$$

Daraus

$$K_n > 2\,\frac{\sqrt{(n-1)}^{n-1}}{\sqrt{n^n}}\,K_{n-1}$$

$$\left(\frac{\sqrt{n}}{2}\right)^n K_n > \left(\frac{\sqrt{n-1}}{2}\right)^{n-1} K_{n-1}.$$

Setzt man also

$$K_n = \left(\frac{2}{\sqrt{\Theta_n\,n}}\right)^n,$$

so ist

(23) $$\Theta_n^n < \Theta_{n-1}^{n-1},$$

also Θ_n^n eine mit wachsenden n abnehmende Zahl. Zugleich ergiebt sich aus (16)

(24) $$M < \Theta_n\,n\,\sqrt[n]{D}.$$

Für $n=2$ ist K_n gleich dem Flächeninhalt des Kreises mit dem Radius 1, d. h. gleich der Ludolfischen Zahl π, und daraus ergiebt sich

$$\Theta_2 = \frac{2}{\pi} < 0{,}636,\quad \Theta_2^2 < 0{,}404,$$

und es gilt also nach (22) und (23) die für alle Werthe von n, die grösser als 1 sind, gültige Grenzbestimmung:

(25) $$M < n\,\sqrt[n]{0{,}404\,D}\ ^{1)}.$$

[1]) Für specielle Anwendungen ist es nützlich, die Grenze so genau als möglich zu kennen. Dazu dient eine genaue Berechnung des Integrals K_n nach seiner Definition (17), (18), die sich leicht nach verschiedenen Methoden der Integralrechnung, z. B. mittelst des discontinuirlichen Factors von Dirichlet, ausführen lässt:

$$K_n = \frac{\Gamma\left(\frac{1}{2}\right)^n}{\Gamma\left(1+\frac{n}{2}\right)},$$

§. 156.

Anwendung auf algebraische Körper.

Aus dem Minimum für eine positive quadratische Form kann man ein Minimum von Linearformen ableiten, indem man eine positive quadratische Form als Summe von Quadraten von Linearformen auffasst. Darauf beruhen die folgenden Anwendungen auf die Theorie der algebraischen Körper, denen wir einen Hülfssatz vorausschicken:

1. Sind $a_1, a_2, \ldots, a_n$ reelle positive Zahlwerthe, so ist

$$a_1 + a_2 + \cdots + a_n \gtreqless n \sqrt[n]{a_1 a_2 \ldots a_n}. \tag{1}$$

Dieser Satz ist offenbar richtig für $n = 2$, denn es ist $a_1 + a_2 - 2\sqrt{a_1 a_2} = (\sqrt{a_1} - \sqrt{a_2})^2$, also nie negativ. Wir wenden also die vollständige Induction an, indem wir die Formel (1) für $n - 1$ Glieder als schon erwiesen annehmen. Nehmen wir dann an, dass a_n von keinem der übrigen a an Grösse übertroffen wird, so ist

$$a_n \gtreqless \sqrt[n-1]{a_1 a_2 \ldots a_{n-1}} = b,$$

und

$$a_1 + a_2 + \cdots + a_{n-1} \gtreqless (n-1)\, b.$$

Also ist

$$a_1 + a_2 + \cdots + a_n \gtreqless a_n + (n-1)\, b,$$

und folglich

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \gtreqless b + \frac{a_n - b}{n},$$

---

worin $\Gamma(x)$ die Gammafunction bedeutet, für die die Gleichungen

$$\Gamma(x) = (x-1)\, \Gamma(x-1), \quad \Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$$

bestehen, so dass K_n durch rationale Zahlen und durch $\sqrt{\pi}$ ausgedrückt ist.

(Vergl. z. B. Vorlesungen über die Theorie der bestimmten Integrale nach Lejeune-Dirichlet von G. F. Meyer herausgegeben, §. 175. Leipzig 1871).

Daraus ergiebt sich

$$\Theta_n = \frac{4}{n\pi}\, \Gamma\left(1 + \frac{n}{2}\right)^{\frac{2}{n}},$$

was nach den Näherungsformeln für die Γ-Function für grosse Werthe von n nahe mit

$$\frac{2}{\pi e} = 0{,}234 \ldots$$

übereinstimmt. (Minkowski, Crelle, Bd. 107, S. 292).

und nach dem binomischen Satze, da $a_n - b$ nicht negativ ist,

$$\left(\frac{a_1 + a_2 + \cdots + a_n}{n}\right)^n \gtrless b^n + b^{n-1}(a_n - b) = a_n b^{n-1},$$

dies aber fällt mit der zu beweisenden Ungleichung (1) zusammen.

Es sei nun $\omega_1, \omega_2, \ldots, \omega_n$ eine Minimalbasis eines algebraischen Körpers Ω. Es sei ferner φ ein beliebiges ganzes Functional.

Wir nehmen eine Basis von φ an (§. 146):

$$(2) \qquad (\beta_1, \beta_2, \ldots, \beta_n) = \begin{pmatrix} b_{1,1} & \ldots & b_{1,n} \\ \cdot & \cdots & \cdot \\ b_{n,1} & \ldots & b_{n,n} \end{pmatrix} (\omega_1, \omega_2, \ldots, \omega_n),$$

so dass

$$(3) \qquad N_a(\varphi) = \pm \Sigma \pm b_{1,1} \ldots b_{n,n}$$

wird. Aus der mit φ associirten Linearform

$$(4) \qquad \eta = \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n$$

erhalten wir dann alle durch φ theilbaren ganzen Zahlen des Körpers Ω, wenn für die $x_1, x_2, \ldots, x_n$ alle möglichen Combinationen ganzer Zahlen gesetzt werden.

Aus (4) ergeben sich n verschiedene Formen $\eta_1, \eta_2, \ldots, \eta_n$, wenn wir zu den n conjugirten Körpern, $\Omega_1, \Omega_2, \ldots, \Omega_n$ übergehen. Das Quadrat der Determinante dieses Systems von n Formen ist nach §. 147 gleich der Discriminante

$$(5) \qquad \Delta(\beta_1, \beta_2, \ldots, \beta_n) = \pm N_a(\varphi)^2 \Delta,$$

wenn Δ die Grundzahl des Körpers bedeutet.

Die conjugirten Körper $\Omega_1, \Omega_2 \ldots$ können theils reell, theils paarweise conjugirt imaginär sein. Wir bezeichnen, wie früher schon mehrfach, mit $|\omega|$ den absoluten Werth einer reellen oder complexen Grösse und betrachten, indem wir unter $x_1, x_2, \ldots, x_n$ reelle Variable verstehen, die quadratische Form

$$(6) \quad f(x_1, x_2, \ldots, x_n) = |\eta_1|^2 + |\eta_2|^2 + \cdots + |\eta_n|^2 = S\,|\eta|^2.$$

Ist Ω reell, so ist

$$(7) \qquad |\eta|^2 = \eta^2,$$

also das Quadrat einer reellen linearen Form. Wenn aber Ω, Ω' zwei conjugirt imaginäre unter den conjugirten Körpern sind, so sind auch die entsprechenden Linearformen η, η' conjugirt imaginär, und es ist

$$(8) \qquad |\eta|^2 = |\eta'|^2 = \eta\,\eta'$$

die Summe von zwei Quadraten reeller Linearformen. Das Product $\eta\eta'$ tritt dann mit dem Factor 2 in der Function f auf. Daher ist f unter allen Umständen eine positive Form.

Nach (7), (8) lässt sich aber f auch als quadratische Form der Variablen $\eta_1, \eta_2, \ldots, \eta_n$

(9) $$f = F(\eta_1, \eta_2, \ldots, \eta_n) = \sum^{i,k} a_{i,k}\, \eta_i\, \eta_k$$

auffassen, und hierin ist, wenn η_i reell ist, $a_{i,i} = 1$, und wenn η_i, η_k ein conjugirt imaginäres-Paar ist, $a_{i,k} = 1$. Alle übrigen Coëfficienten sind $= 0$. Die Determinante von F ist also $= \pm 1$, weil in jeder Zeile und in jeder Colonne nur ein von Null verschiedenes Element mit dem Werthe 1 vorkommt. Nach Bd. I, §. 56 ist die Determinante der Form f gleich dem Product der Determinante von F und dem Quadrate der Determinante der linearen Formen η, also nach (5)

(10) $$= \pm [N_a(\varphi)]^2 \Delta,$$

wo das Zeichen so zu wählen ist, dass der Werth positiv ausfällt.

Nach §. 155, (24) kann man nun für die x_i solche ganze rationale Zahlen setzen, dass

(11) $$f(x_1, x_2, \ldots, x_n) < \Theta_n\, n \sqrt[n]{\pm \Delta N_a(\varphi)^2}$$

wird, worin Θ_n, wenn n grösser als 1 ist, ein echter Bruch und immer kleiner als $\sqrt[3]{0{,}404}$ ist. Setzt man diese Werthe von x_i in (4) ein, so geht η in eine ganze durch φ theilbare Zahl β über, und wir haben also damit den Satz:

2. Ist φ irgend ein ganzes Functional in Ω, so giebt es eine durch φ theilbare ganze Zahl β in Ω von der Eigenschaft, dass

(12) $$S|\eta|^2 < \Theta_n\, n \sqrt[n]{\pm \Delta\, [N_a(\varphi)]^2}$$

wird, worin Δ die Grundzahl des Körpers und $\pm \Delta$ positiv ist.

Das Product der conjugirten Werthe η ist gleich der Norm von η, und daher ist nach dem Hülfssatze 1. [mit Rücksicht auf (7) und (8)]

(13) $$n \sqrt[n]{[N(\eta)]^2} \gtreqless S|\eta|^2,$$

und also folgt nach (12) die auf die absoluten Werthe bezügliche Ungleichung:

(14) $$N(\eta)^2 < \Theta_n^n\, [N_a(\varphi)]^2 \Delta.$$

Da nun η durch φ theilbar ist, so können wir

$$\varepsilon\eta = \varphi\psi, \quad \pm N(\eta) = N_a(\varphi)\, N_a(\psi)$$

setzen, worin ψ ein ganzes Functional, ε eine Einheit ist, und erhalten aus (14)

$$(15) \qquad N_a(\psi) < \sqrt{\pm 0{,}404\,\Delta}.$$

Da wir für φ jedes ganze Functional setzen können, so kann ψ ein Repräsentant eines Ideals einer beliebigen Classe sein, und wir haben damit den wichtigen Satz bewiesen:

3. **In jeder Idealclasse können wir einen Repräsentanten finden, dessen Norm kleiner als die Quadratwurzel aus dem absoluten Werthe der Grundzahl des Körpers ist.**

Die im §. 153 zum Beweise der Endlichkeit der Classenzahl benutzte obere Grenze für die Norm eines Ideals einer Classe wird hierdurch in viel schärferer Weise bestimmt.

Aber noch einen anderen sehr bemerkenswerthen Schluss gestattet die Ungleichung (15). Da nämlich $N_a(\psi)$ eine positive ganze Zahl, also mindestens gleich 1 ist, so geht aus (15) hervor, dass, abgesehen von dem Falle $n = 1$, Δ absolut grösser als 1 sein muss, dass es also ausser dem Körper der rationalen Zahlen keinen Körper giebt, dessen Grundzahl ± 1 wäre. Dies ist der von Minkowski zuerst erbrachte, früher lange vergeblich gesuchte Beweis dieses wichtigen Satzes[1]).

§. 157.

Primfactoren der natürlichen Primzahlen.

Eine genauere Untersuchung der im §. 146 erklärten Basisform τ von $\mathfrak{o}$ des Körpers Ω soll uns nun das Mittel geben,

---

[1]) In einem Briefe an Hermite (Comptes rendus d. Pariser Akademie, 26. Januar 1891) und auch in dem oben erwähnten Buche findet Minkowski eine weit engere Grenze, indem er nicht nur das Minimum der quadratischen Formen, sondern noch anderer Functionen betrachtet, wie $\eta_1^p + \eta_2^p + \cdots + \eta_n^p$, worin p eine beliebige positive Zahl ist, die nicht einmal ganz zu sein braucht. Für $p = 1$ ergiebt sich, wenn $n - \nu$ die Anzahl der conjugirt imaginären Paare ist:

$$N_a(\psi) < \left(\frac{4}{\pi}\right)^{n-\nu} \frac{1 \cdot 2 \cdot 3 \ldots n}{n^n} \sqrt{\pm \Delta}.$$

Daraus lassen sich noch weitere Schlüsse ziehen, wie die: Die Grundzahl eines quadratischen Körpers muss grösser als 4 oder keiner als — 2 sein; die Grundzahl eines cubischen Körpers muss grösser als 20 oder kleiner als — 12 sein etc.

jede beliebig gegebene natürliche Primzahl p in ihre Primfactoren wirklich zu zerlegen, und damit alle Primideale des Körpers $\mathfrak{K}$, oder wenigstens Repräsentanten aller Primideale wirklich darzustellen [1]).

Es sei $\mathfrak{p}$ ein beliebiges Primideal vom Grade f, so dass

(1) $$N(\mathfrak{p}) = p^f$$

ist, worin p eine natürliche Primzahl bedeutet, die durch den Primfactor $\mathfrak{p}$ theilbar ist. f ist ein positiver Exponent $\lesseqgtr n$. Die kleinste ganze rationale Zahl, die durch $\mathfrak{p}$ theilbar ist, ist p, und jede andere ganze rationale Zahl, die durch $\mathfrak{p}$ theilbar ist, ist daher auch durch p theilbar (§. 138).

Wir müssen nun auch Congruenzen mit dem Modul $\mathfrak{p}$ zwischen ganzen Functionen beliebiger Variablen mit Coëfficienten in $\mathfrak{o}$ betrachten und bemerken, dass zwei solche Functionen nach §. 143, 2. dann und nur dann congruent sind, wenn die entsprechenden Coëfficienten congruent sind.

Den Körper der rationalen Zahlen bezeichnen wir mit R und nennen demnach eine Function mit rationalen Coëfficienten auch eine Function in R.

Die Basisform von $\mathfrak{o}$

(2) $$\tau = \omega_1 t_1 + \omega_2 t_2 + \cdots + \omega_n t_n$$

genügt, wie wir im §. 146 gesehen haben, einer Gleichung n^{ten} Grades $F(\tau) = 0$, deren Coëfficienten ganze rationale Functionen von $t_1, t_2, \ldots, t_n$ sind. Es ist also $F(\tau)$ jedenfalls durch $\mathfrak{p}$ theilbar, und daraus folgt, dass es ganze Functionen $\Phi(t)$ in R giebt, die ausser t irgend welche Variable enthalten können, die durch die Substitution $t = \tau$ in durch $\mathfrak{p}$ theilbare Functionale in $\mathfrak{o}$ übergehen, die also der Congruenz

(3) $$\Phi(\tau) \equiv 0 \pmod{\mathfrak{p}}$$

genügen, und wir werden also sagen können, τ ist eine Wurzel der Congruenz

(4) $$\Phi(t) \equiv 0 \pmod{\mathfrak{p}}.$$

Die Function Φ wird gewiss die Variablen $t_1, t_2, \ldots, t_n$ enthalten müssen; sie kann aber auch noch andere Variable ent-

---

[1]) Wir folgen hier einer Arbeit von Hensel: „Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Theiler der Discriminante“ (Crelle's Journ., Bd. 113). Zu erwähnen sind auch die anderen Arbeiten von Hensel, Ebend., Bd. 101, 104, 105, 113.

halten, und wenn wir also die Variablen von Φ mit $t, u_1, u_2, \ldots$ bezeichnen, werden wir auch setzen

$$(5) \qquad \Phi(t) = \Phi(t, u_1, u_2, \ldots),$$

oder kürzer $\Phi\,(t, u)$, und diese Function enthält ganze rationale Zahlencoëfficienten. Wenn wir die Function $\Phi(t)$ in die p^{te} Potenz erheben, und die Formel §. 150, 4. anwenden, so folgt aus der Congruenz (3) eine neue Congruenz

$$(6) \qquad \Phi(\tau^p, u_1^p, u_2^p, \ldots) \equiv 0 \pmod{\mathfrak{p}}.$$

Ebenso ist aber auch

$$(7) \qquad \tau^p \equiv \omega_1^p t_1^p + \omega_2^p t_2^p + \cdots + \omega_n^p t_n^p.$$

Wenn wir dies in die Congruenz (6) substituiren, so entsteht eine durch $\mathfrak{p}$ theilbare Function, in der die Variablen $u_1, u_2, \ldots$, unter denen ja die $t_1, t_2, \ldots, t_n$ mit enthalten sind, nur in der p^{ten} Potenz vorkommen. Die Congruenz muss also richtig bleiben, wenn wir die $u_1^p, u_2^p, \ldots$ und also auch die $t_1^p, t_2^p, \ldots, t_n^p$ durch unabhängige Variable $u_1, u_2, \ldots t_1, t_2, \ldots, t_n$ ersetzen (§. 143).

Setzen wir demnach

$$(8) \qquad \tau_1 = \omega_1^p t_1 + \omega_2^p t_2 + \cdots + \omega_n^p t_n,$$

so ergiebt sich aus (6)

$$\Phi(\tau_1, u_1, u_2, \ldots) \equiv 0 \pmod{\mathfrak{p}},$$

und folglich ist τ_1 auch eine Wurzel der Congruenz (4).

Dieses nämliche Verfahren lässt sich wiederholt anwenden, und wir finden, dass auch

$$\tau_2 = \omega_1^{p^2} t_1 + \omega_2^{p^2} t_2 + \cdots + \omega_p^{p^2} t_n$$

Wurzel der Congruenz (4) ist, u. s. f.

Wenn wir also ein System von Formen τ_r definiren durch

$$(9) \qquad \tau_r = \omega_1^{p^r} t_1 + \omega_2^{p^r} t_2 + \cdots + \omega_n^{p^r} t_n$$

für beliebige positive Exponenten r, so sind alle diese Grössen τ_r zugleich Wurzeln der Congruenz (4). Es ist noch die Frage zu beantworten, wie viele von diesen Formen τ_r von einander verschieden sind.

Nach §. 150, (4) ist sicher

$$\tau_r \equiv \tau_{r'} \pmod{\mathfrak{p}},$$

wenn

$$r \equiv r' \pmod{f}$$

ist, und folglich giebt es unter den τ_r gewiss nicht mehr als f nach dem Modul $\mathfrak{p}$ verschiedene

$$(10) \qquad \tau, \tau_1, \tau_2, \ldots, \tau_{f-1}.$$

Dass diese Formen aber wirklich von einander verschieden sind, ergiebt sich daraus, dass wir (nach §. 145, 150) für die Variablen $t_1, t_2, \ldots, t_n$ solche ganze rationale Zahlen setzen können, dass τ in eine primitive Wurzel γ des Primideals $\mathfrak{p}$ übergeht. Durch dieselbe Substitution werden die Grössen (10)

(11) $$\equiv \gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{f-1}} \pmod{\mathfrak{p}},$$

die nach dem Modul $\mathfrak{p}$ alle von einander verschieden sind. Es können also auch nicht zwei der Formen (10) nach dem Modul $\mathfrak{p}$ congruent sein, weil sonst auch die beiden entsprechenden Zahlen (11) congruent ausfallen würden.

Dies fassen wir als Satz so zusammen:

1. Jede Congruenz (4), deren eine Wurzel $t = \tau$ ist, hat die f verschiedenen Wurzeln

$$\tau, \tau_1, \tau_2, \ldots, \tau_{f-1}.$$

Hiernach können wir, indem wir $\Phi(t)$ durch $t - \tau$ algebraisch dividiren,

$$\Phi(t) \equiv (t - \tau)\, \Phi_1(t) \pmod{\mathfrak{p}}$$

setzen, und $\tau_1, \tau_2, \ldots, \tau_{f-1}$ sind Wurzeln von $\Phi_1(t) \equiv 0$, worin aber $\Phi_1(t)$ noch nicht rationale Coëfficienten, sondern Coëfficienten in $\mathfrak{o}$ hat. Dividiren wir $\Phi_1(t)$ wieder durch $t - \tau_1$, und fahren so fort, so folgt endlich, wenn wir also nun die Function f^{ten} Grades

(12) $$\Pi(t) = (t - \tau)(t - \tau_1) \ldots (t - \tau_{f-1})$$

setzen,

(13) $$\Phi(t) \equiv \Pi(t)\, \Phi_0(t) \pmod{\mathfrak{p}},$$

worin $\Phi_0(t)$ eine ganze Function mit Coëfficienten in $\mathfrak{o}$ ist.

Die Function $\Pi(t)$ hängt von den Variablen $t, t_1, \ldots, t_n$ ab, und um dies auszudrücken, setzen wir

$$\Pi(t) = \Pi(t, t_1, \ldots, t_n).$$

Die Coëfficienten dieser Form sind Zahlen in $\mathfrak{o}$, und es lässt sich noch nachweisen, dass sie mit ganzen rationalen Zahlen nach dem Modul $\mathfrak{p}$ congruent sind. Dieser Beweis ergiebt sich durch Erheben in die p^{te} Potenz:

$$[\Pi(t)]^p \equiv (t^p - \tau^p)(t^p - \tau_1^p) \ldots (t^p - \tau_{f-1}^p).$$

Nun ist aber nach (9)

$$\tau_r^p \equiv \omega_1^{p^{r+1}}\, t_1^p + \omega_2^{p^{r+1}}\, t_2^p + \cdots + \omega_n^{p^{r+1}}\, t_n^p \pmod{\mathfrak{p}},$$

und wir erhalten also τ_r^p aus τ_{r+1}, wenn wir t_i durch t_i^p ersetzen,

und τ_f ist congruent mit τ. Demnach erhalten wir die Congruenz:

$$[\Pi(t, t_1, t_2, \ldots, t_n)]^p \equiv \Pi(t^p, t_1^p, t_2^p, \ldots, t_n^p) \pmod{\mathfrak{p}}.$$

Damit ist nach §. 150, 4. der Satz bewiesen:

2. Die Form

$$\Pi(t) = (t - \tau)(t - \tau_1) \ldots (t - \tau_{f-1})$$

ist nach dem Modul $\mathfrak{p}$ mit einer ganzen und homogenen Form f^{ten} Grades in R der Variablen $t, t_1, t_2, \ldots, t_n$ congruent.

Diese ganze rationale Form, deren Coëfficienten bis auf Vielfache der Primzahl p völlig bestimmt sind, wollen wir mit $P(t)$ bezeichnen.

Dann folgt aus (13)

(14) $$\Phi(t) \equiv P(t)\, \Phi_0(t) \pmod{\mathfrak{p}},$$

und da nun $\Phi(t)$ eine ganze Function in R ist, so ergiebt sich durch Erheben zur Potenz p:

$$\left.\begin{aligned} \Phi(t^p, u^p) &\equiv P(t^p, u^p)\;\; \Phi_0(t^p, u^p) \\ [\Phi(t, u)]^p &\equiv [P(t, u)]^p\, [\Phi_0(t, u)]^p \end{aligned}\right\} \pmod{\mathfrak{p}}.$$

Weil aber die linken Seiten nach dem Modul $\mathfrak{p}$ congruent sind, so folgt

$$[P(t)]^p\, [\Phi_0(t, u)^p - \Phi_0(t^p, u^p)] \equiv 0 \pmod{\mathfrak{p}},$$

und daraus, da $P(t)$ nicht durch $\mathfrak{p}$ theilbar ist (weil der Coëfficient von t^f den Werth 1 hat):

(15) $$[\Phi_0(t, u)]^p \equiv \Phi_0(t^p, u^p),$$

woraus nach §. 150, 4. hervorgeht, dass auch $\Phi_0(t)$ mit einer ganzen rationalen Form nach dem Modul $\mathfrak{p}$ congruent ist.

Demnach können wir in (14) auch $\Phi_0(t)$ als ganze Form in R annehmen, und dann muss nach §. 140, 3. die Congruenz (14) nicht nur für den Modul $\mathfrak{p}$, sondern für den Modul p bestehen. Daraus erhalten wir den Satz:

3. Unter den Formen $\Phi(t)$, die für $t = \tau$ in ein durch $\mathfrak{p}$ theilbares Functional übergehen, ist $P(t)$ vom Grade f in Bezug auf t die Form niedrigsten Grades, und wenn $\Phi(t)$ eine beliebige unter ihnen ist, so lässt sich eine ganze Function $\Phi_0(t)$ in R so bestimmen, dass

(15) $$\Phi(t) \equiv P(t)\, \Phi_0(t) \pmod{p}$$

wird.

Lassen wir in $\Phi(t)$ und $\Phi_0(t)$ Glieder weg, deren Coëfficienten durch p theilbar sind, so ist der Grad von $\Phi(t)$ in Bezug auf t um f grösser als der Grad von $\Phi_0(t)$.

$P(t)$ ist eine ganze Function in R der Variablen $t, t_1, t_2, \ldots, t_n$, die durch die Substitution $t = \tau$ in ein durch $\mathfrak{p}$ theilbares Functional übergeht, die natürlich nicht mehr in R enthalten ist.

Die Bedeutung dieser Form $P(t)$ tritt nun noch deutlicher hervor, wenn wir den Satz beweisen:

4. Der Primfactor $\mathfrak{p}$ ist der grösste gemeinschaftliche Theiler von p und $P(\tau)$.

Dazu haben wir nur nachzuweisen, dass, wenn p durch $\mathfrak{p}\mathfrak{p}_1$ theilbar ist, wo $\mathfrak{p}$, $\mathfrak{p}_1$ zwei gleiche oder verschiedene Primfactoren sind, $P(\tau)$ zwar durch $\mathfrak{p}$, nicht aber durch $\mathfrak{p}\mathfrak{p}_1$ theilbar ist.

Nach §. 143, 3. existirt immer eine Zahl ξ in $\mathfrak{o}$, die zwar durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}\mathfrak{p}_1$ theilbar ist. Diese Zahl wird die Form haben

$$(16) \qquad \xi = a_1 \omega_1 + a_2 \omega_2 + \cdots + a_n \omega_n,$$

worin die $a_1, a_2, \ldots, a_n$ ganze rationale Zahlen sind, und geht also aus der Form τ hervor durch die Substitution

$$(17) \qquad (t_1, t_2, \ldots, t_n) = (a_1, a_2, \ldots, a_n).$$

Wenn wir dieselbe Substitution in den in (9) definirten Formen τ_r machen, so geht τ_r in eine Zahl ξ_r über, die nach dem Fermat'schen Satze der Congruenz

$$\xi^{p^r} \equiv \xi_r \pmod{\mathfrak{p}}$$

genügt und also sicher auch durch $\mathfrak{p}$ theilbar ist.

Wenn wir daher in der Form

$$\Pi(t) = (t - \tau)(t - \tau_1) \ldots (t - \tau_{f-1})$$

$\tau_r + \xi_r$ an Stelle von τ_r setzen, so bleibt diese Form mit sich selbst nach dem Modul $\mathfrak{p}$ congruent. Diese Substitution kommt aber darauf hinaus, dass wir $t_1 + a_1, t_2 + a_2, \ldots, t_n + a_n$ an Stelle von $t_1, t_2, \ldots, t_n$ substituiren, und wir erhalten demnach

$$\Pi(t, t_1 + a_1, \ldots, t_n + a_n) \equiv \Pi(t, t_1, \ldots, t_n) \pmod{\mathfrak{p}},$$

nnd wenn wir Π durch die congruente Form P ersetzen

$$P(t, t_1 + a_1, \ldots, t_n + a_n) \equiv P(t, t_1, \ldots, t_n) \pmod{\mathfrak{p}}.$$

Da aber die Form P lauter **rationale** Coëfficienten hat, so muss die letztere Congruenz auch nach dem Modul p stattfinden, also

$$(18)\quad P(t, t_1 + a_1, \ldots, t_n + a_n) \equiv P(t, t_1, \ldots, t_n) \pmod{p}.$$

Diese Congruenz besteht für variable $t, t_1, \ldots, t_n$.

Nehmen wir nun an, dass, entgegen dem zu beweisenden Satze, $P(\tau)$ durch $\mathfrak{p}\,\mathfrak{p}_1$ theilbar sei, so besteht die Congruenz

$$(19)\quad P(\tau, t_1, \ldots, t_n) \equiv 0 \pmod{\mathfrak{p}\,\mathfrak{p}_1},$$

und diese bleibt richtig, wenn für die unabhängigen Variablen $t_1, t_2, \ldots, t_n$ die Substitution $t_1 + a_1, t_2 + a_2, \ldots, t_n + a_n$ gemacht wird, und da hierdurch τ in $\tau + \xi$ übergeht, so folgt

$$(20)\quad P(\tau + \xi, t_1 + a_1, \ldots, t_n + a_n) \equiv 0 \pmod{\mathfrak{p}\,\mathfrak{p}_1}.$$

Machen wir andererseits in der Congruenz (18) die Substitution $t = \tau + \xi$, so folgt

$$(21)\quad P(\tau + \xi, t_1, \ldots, t_n) = P(\tau + \xi) \equiv 0 \pmod{\mathfrak{p}\,\mathfrak{p}_1}.$$

Nehmen wir nun zunächst an, $\mathfrak{p}_1$ sei von $\mathfrak{p}$ verschieden, dann können wir so schliessen.

Wir setzen in (21) $t_1 = t_2 = \cdots = t_n = 0$, also auch $\tau = 0$. Dadurch aber geht $P(t)$ in t^f über (abgesehen von Vielfachen von p), und es ergiebt sich aus (21)

$$\xi^f \equiv 0 \pmod{\mathfrak{p}\,\mathfrak{p}_1},$$

was aber der Annahme widerspricht, dass ξ nicht durch $\mathfrak{p}_1$ theilbar sein soll.

Ist aber $\mathfrak{p}_1 = \mathfrak{p}$, so ordnen wir (21) nach Potenzen von ξ und erhalten

$$(22)\quad P(\tau + \xi) = P(\tau) + \xi P'(\tau) + \frac{\xi^2}{2} P''(\tau) \ldots,$$

wenn $P'(t), P''(t), \ldots$ die Derivirten von $P(t)$ sind, wobei zu beachten ist, dass die Formen

$$\frac{1}{2} P''(t), \frac{1}{2.3} P'''(\tau), \ldots$$

trotz der scheinbaren Nenner ganze Formen in R sind. Da nun nach (19) und (21) $P(\tau + \xi)$ und $P(\tau)$ durch $\mathfrak{p}^2$ theilbar sind, und ebenso nach Voraussetzung $\xi^2, \xi^3, \ldots$, während ξ nicht durch $\mathfrak{p}^2$ theilbar ist, so folgt aus (22)

$$P'(\tau) \equiv 0 \pmod{\mathfrak{p}},$$

woraus wegen

$$P(t) \equiv \Pi(t) \pmod{\mathfrak{p}}$$

nach der Bedeutung (12) von $\Pi(t)$ folgt:

$$\Pi'(\tau) \equiv (\tau - \tau_1)(\tau - \tau_2) \ldots (\tau - \tau_{f-1}) \equiv 0 \pmod{\mathfrak{p}}.$$

Dies ist aber unmöglich, weil die $\tau, \tau_1, \ldots \tau_{f-1}$, wie wir gesehen haben, nach dem Modul $\mathfrak{p}$ incongruent sind. Damit ist also unser Satz 4. vollständig bewiesen. Wir können hiernach, wenn x, y zwei neue Variable bedeuten, ein Functional π des Ideals $\mathfrak{p}$ bilden:

(23) $$\pi = xp + yP(\tau).$$

Wir betrachten nun ganze Formen $\Phi(t)$ in R, die durch die Substitution $t = \tau$ nicht nur durch $\mathfrak{p}$, sondern durch die natürliche Primzahl p theilbar werden, also der Congruenz

(24) $$\Phi(\tau) \equiv 0 \pmod{p}$$

genügen. Die Primzahl p möge folgendermaassen in ihre Primfactoren in Ω zerlegt sein:

(25) $$p = \mathfrak{p}\,\mathfrak{p}_1\,\mathfrak{p}_2 \ldots,$$

worin

$$\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$$

gleiche oder verschiedene Primideale der Grade

$$f, f_1, f_2, \ldots$$

sind. Diesen Primfactoren entspricht (nach dem Satze 3.) eine Reihe ganzer rationaler Formen

$$P(t),\ P_1(t),\ P_2(t), \ldots$$

der Grade $f, f_1, f_2, \ldots$, und wenn etwa $\mathfrak{p}$ mit $\mathfrak{p}_1$ identisch ist, so ist auch $P(t)$ mit $P_1(t)$ identisch. Wenn man in (25) rechts und links die Norm nimmt, und die Formel $N(\mathfrak{p}) = p^f$ berücksichtigt [§. 140, (3), §. 151, (3)], so folgt

(26) $$n = f + f_1 + f_2 + \cdots$$

Wenn nun $\Phi(t)$ eine der Bedingung (24) genügende ganze rationale Form ist, so folgt aus dem Satze 3.

(27) $$\Phi(t) \equiv P(t)\,\Phi_1(t) \pmod{p},$$

worin $\Phi_1(t)$ eine ganze Function in R ist, die der Bedingung

$$P(\tau)\,\Phi_1(\tau) \equiv 0 \pmod{\mathfrak{p}\,\mathfrak{p}_1\,\mathfrak{p}_2 \ldots}$$

genügt. Nach dem Satze 4. folgt hieraus

(28) $$\Phi_1(\tau) \equiv 0 \pmod{\mathfrak{p}_1\,\mathfrak{p}_2 \ldots},$$

und daraus schliesst man wieder nach Satz 3. (auf $\mathfrak{p}_1$ angewandt)

$$\Phi_1(t) \equiv P_1(t)\, \Phi_2(t) \pmod{p}.$$

Hierin lässt sich dieselbe Betrachtung wiederholen, die zu der Congruenz

$$\Phi_2(t) \equiv 0 \pmod{\mathfrak{p}_2 \ldots}$$

führt, woraus wieder nach 3.

$$\Phi_2(t) \equiv P_2(t)\, \Phi_3(t) \pmod{p}$$

zu schliessen ist. Fährt man damit fort, bis alle Primfactoren von p berücksichtigt sind, so ergiebt sich der folgende Satz:

5. Ist $\Phi(t)$ eine ganze Function in R, die durch die Substitution $t = \tau$ durch p theilbar wird, so lässt sich eine andere ganze Function $\Phi_0(t)$ in R so bestimmen, dass

$$\Phi(t) \equiv \Phi_0(t)\, P(t)\, P_1(t)\, P_2(t) \ldots \pmod{p} \tag{29}$$

wird.

Das Product $P(t)\, P_1(t)\, P_2(t) \ldots$ ist vom Grade $n = f + f_1 + f_2 + \cdots$ und ist die ganze rationale Form niedrigsten Grades, die durch die Substitution $t = \tau$ durch p theilbar wird.

Zu den im Satze 5. vorkommenden Functionen $\Phi(t)$ gehört auch die ganze Function n^{ten} Grades

$$F(t) = N(t - \tau),$$

die für $t = \tau$ verschwindet. Für diese Function wird $\Phi_0(t)$ von t unabhängig, und da sowohl in $F(t)$ als in $P(t), P_1(t), P_2(t) \ldots$ die höchste Potenz von t den Coëfficienten 1 hat, so wird $\Phi_0(t) = 1$. Es gilt also die Congruenz

$$N(t - \tau) \equiv P(t)\, P_1(t)\, P_2(t) \ldots \pmod{p}. \tag{30}$$

Fassen wir in der Zerlegung (25) der Primzahl p die gleichen Primfactoren zu Potenzen zusammen, so können wir, wenn $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ verschiedene Primideale der Grade $f_1, f_2, \ldots$ sind, die positiven Exponenten $e_1, e_2, \ldots$ so annehmen, dass

$$p = \mathfrak{p}_1^{e_1}\, \mathfrak{p}_2^{e_2} \ldots, \tag{31}$$

und

$$n = e_1 f_1 + e_2 f_2 + \cdots \tag{32}$$

wird. Die Formel (30) nimmt dann die Gestalt an

$$N(t - \tau) \equiv [P_1(t)]^{e_1}\, [P_2(t)]^{e_2} \ldots \pmod{p}. \tag{33}$$

§. 158.

Dedekind's Satz über die Körperdiscriminante.

Die in der Discriminante Δ des Körpers Ω aufgehenden natürlichen Primzahlen haben in Bezug auf ihre Zerlegung in Primfactoren einen besonderen Charakter, über den ein Satz von Dedekind die bündigste Auskunft giebt, zu dessen Ableitung wir jetzt schreiten [1]).

Wir bilden nach §. 145, 2. die Potenzen der Basisform

$$\tau = t_1 \omega_1 + t_2 \omega_2 + \cdots + t_n \omega_n,$$

und erhalten die Ausdrücke:

$$(1) \qquad \tau^k = u_{1,k} \omega_1 + u_{2,k} \omega_2 + \cdots + u_{n,k} \omega_n,$$

worin die $u_{i,k}$ ganze rationale Functionen der Variablen $t_1, t_2, \ldots, t_n$ sind. Wir setzen wie oben

$$(2) \qquad F(t) = N(t - \tau),$$

so dass $F(\tau) = 0$ ist. Nun bilden wir nach §. 144 die Discriminante

$$(3) \qquad \Delta(1, \tau, \tau^2, \ldots, \tau^{n-1}) = (-1)^{\frac{n(n-1)}{2}} NF'(\tau),$$

wofür sich nach (1) der Werth ΔU^2 ergiebt, wenn Δ die Körperdiscriminante und

$$(4) \qquad U = \begin{vmatrix} u_{1,0}, & u_{2,0}, & \ldots, & u_{n,0} \\ u_{1,1}, & u_{2,1}, & \ldots, & u_{n,1} \\ \cdot & \cdot & \cdot & \cdot \\ u_{1,n-1}, & u_{2,n-1}, & \ldots, & u_{n,n-1} \end{vmatrix},$$

also eine ganze Function in R ist.

Wir müssen nachweisen, dass die Form U eine Einheit ist. Angenommen, es gehe in U irgend eine Primzahl p auf, so können wir, wie schon im §. 147 bewiesen ist, ein System ganzer Functionen $y_0, y_1, \ldots, y_{n-1}$ in R, die nicht alle durch p theilbar sind, so bestimmen, dass für $i = 1, 2, \ldots, n$

$$y_0 u_{i,0} + y_1 u_{i,1} + \cdots + y_{n-1} u_{i,n-1} \equiv 0 \pmod{p}$$

wird. Dann aber ergiebt sich aus (1)

$$y_0 + y_1 \tau + \cdots + y_{n-1} \tau^{n-1} \equiv 0 \pmod{p}.$$

[1]) Dedekind, „Ueber die Discriminanten endlicher Körper" im XXIX. Bande der Abhandlungen der Gesellschaft der Wissenschaften in Göttingen (1882).

Dies widerspricht aber dem Satze 5. des vorigen Paragraphen, nach dem τ nach einem Primzahlmodul p keiner Congruenz von niedrigerem als n^{tem} Grade genügen kann.

Demnach ergiebt sich aus (3), dass die Grundzahl Δ des Körpers, vom Vorzeichen abgesehen, die absolute Norm der Function $F'(\tau)$ ist, dass also

(5) $$\pm \Delta = N_a[F'(\tau)]$$

zu setzen ist.

Wenn nun statt der ω_i eine andere Basis ω'_i von $\mathfrak{o}$ zu Grunde gelegt wird, so tritt an Stelle von τ eine andere Form

(6) $$\tau' = \omega'_1 t_1 + \omega'_2 t_2 + \cdots + \omega'_n t_n,$$

wofür wir auch setzen können

(7) $$\tau' = \omega_1 t'_1 + \omega_2 t'_2 + \cdots + \omega_n t'_n,$$

und darin sind die ω'_i mit den ω_i durch eine lineare Substitution mit der Determinante ± 1 verbunden (§. 145):

(8) $$(\omega'_1, \omega'_2, \ldots, \omega'_n) = C\,(\omega_1, \omega_2, \ldots, \omega_n).$$

Führt man diese Substitution in (6) aus, und ordnet nach $\omega_1, \omega_2, \ldots, \omega_n$, so ergiebt sich

(9) $$(t'_1, t'_2, \ldots, t'_n) = C_1\,(t_1, t_2, \ldots, t_n),$$

wenn C_1 die transponirte Substitution von C ist (§. 37). Bildet man nun die Function $F(t)$ für die Function τ', so mag sich $F_1(t)$ ergeben; die Ableitung für $t = \tau'$ sei $F'_1(\tau')$. Setzen wir nun

$$F'(\tau) = \Psi(t_1, t_2, \ldots, t_n),$$

so ist Ψ eine ganze Function in R, und es ergiebt sich wegen (7)

$$F'_1(\tau') = \Psi(t'_1, t'_2, \ldots, t'_n).$$

Da die Substitution (9) umkehrbar ist, so folgt hieraus, dass die beiden Functionale $F'(\tau')$ und $F'_1(\tau')$ gegenseitig durch einander theilbar sind (§. 143), und dass sie mithin associirt sind.

Die Function $F'(\tau)$, deren absolute Norm gleich dem absoluten Werthe der Grundzahl ist, nennen wir daher das Grundfunctional, und das durch $F'(\tau)$ repräsentirte Ideal das Grundideal des Körpers Ω. Nun sei $\mathfrak{p}^e$ die höchste Potenz des Primideals $\mathfrak{p}$, die in p aufgeht, und $e \gtreqless 1$, dann können wir nach 5. des vorigen Paragraphen

(10) $$F(t) \equiv P(t)^e\,\Phi(t) \pmod{\mathfrak{p}}$$

setzen, worin $\Phi(t)$ eine ganze Function in R von der Beschaffenheit ist, dass $\Phi(\tau)$ nicht durch $\mathfrak{p}$ theilbar ist. Aus (10) aber

folgt, indem wir die Ableitung nach t bilden, was offenbar gestattet ist:

$$F'(t) \equiv e\,[P(t)]^{e-1}\,P'(t)\,\Phi(t) + [P(t)]^e\,\Phi'(t) \pmod p.$$

Setzen wir hierin $t = \tau$, so geht $P'(t)$ in eine durch $\mathfrak{p}$ untheilbare Form $P'(\tau)$ über (was wir schon im Beweis von §. 157, 4. gezeigt und benutzt haben) und wir erhalten

(11) $$F'(\tau) \equiv e\,P(\tau)^{e-1}\,P'(\tau)\,F_1(\tau) \pmod{\mathfrak{p}^e}.$$

Nun ist (nach §. 157, 4.) $P(\tau)$ durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbar, $P'(\tau)$ und $\Phi(\tau)$ sind durch $\mathfrak{p}$ nicht theilbar, und so giebt uns also die Formel (11) den Beweis des folgenden Satzes:

1. Ist $\mathfrak{p}$ ein beliebiges Primideal, p die durch $\mathfrak{p}$ theilbare natürliche Primzahl, und $\mathfrak{p}^e$ die höchste in p aufgehende Potenz von $\mathfrak{p}$, so ist die Grundform $F'(\tau)$ allemal theilbar durch $\mathfrak{p}^{e-1}$; ist ferner der Exponent e nicht theilbar durch p, so ist $F'(\tau)$ nicht theilbar durch $\mathfrak{p}^e$; ist aber e theilbar durch p, so ist $F'(\tau)$ theilbar durch $\mathfrak{p}^e$ und vielleicht durch noch höhere Potenzen von $\mathfrak{p}$.

Wenn e grösser als 1 ist, so ist hiernach $F'(\tau)$ durch $\mathfrak{p}$ theilbar, und folglich ist $N_\alpha[F'(\tau)]$ und also auch die Grundzahl $\varDelta$ durch p theilbar.

Wenn aber alle Primideale $\mathfrak{p}$ nur in erster Potenz in p aufgehen, so ist $F'(\tau)$ relativ prim zu p. Zerlegt man also $F'(\tau)$ in seine Primfactoren, so kommt darunter keiner vor, dessen Norm eine Potenz von p ist, folglich ist auch $N_\alpha[F'(\tau)]$ und $\varDelta$ durch p nicht theilbar. Daraus folgt dann der Satz:

2. Eine natürliche Primzahl p ist dann und nur dann im Körper Ω durch das Quadrat eines Primfactors theilbar, wenn p in der Grundzahl von Ω aufgeht.

Aus diesen Betrachtungen können wir noch andere wichtige Schlüsse ziehen.

Wenn wir das System der linearen Gleichungen (1) in Bezug auf $\omega_1, \omega_2, \ldots, \omega_n$ auflösen, so erhalten wir Ausdrücke mit dem Nenner U, der, wie wir gesehen haben, eine Einheit ist. Substituirt man diese Ausdrücke in

(12) $$\omega = x_1\,\omega_1 + x_2\,\omega_2 + \cdots + x_n\,\omega_n,$$

worin die $x_1, x_2, \ldots, x_n$ ganze rationale Zahlen oder ganze rationale Functionale sind, so erhält man einen Ausdruck von der Form

$$(13) \qquad \omega = A_0 + A_1 \tau + A_2 \tau^2 + \cdots + A_{n-1} \tau^{n-1},$$

worin die $A_0, A_1, \ldots, A_{n-1}$ gleichfalls ganze rationale Functionale bedeuten. Nach §. 145, 2. wird aber in dieser Form jede ganze Zahl und jedes ganze Functional des Körpers Ω dargestellt, und wir können daher den Satz aussprechen:

3. Die Potenzen

$$1, \tau, \tau^2, \ldots, \tau^{n-1}$$

bilden eine Basis der ganzen Functionale des Körpers Ω.

Statt der Potenzen von τ können auch die Functionen

$$F_0, F_1, F_2, \ldots, F_{n-1}$$

als Elemente der Basis eingeführt werden, die durch die Gleichung

$$(14) \qquad \frac{F(t)}{t - \tau} = t^{n-1} F_0(\tau) + t^{n-2} F_1(\tau) + \cdots + F_{n-1}(\tau)$$

definirt sind, die, wie schon im §. 4 des ersten Bandes gezeigt ist, wenn

$$F(t) = t^n + a_1 t^{n-1} + \cdots + a_n$$

ist, den Ausdruck haben:

$$(15) \qquad \begin{aligned} F_0(t) &= 1 \\ F_1(t) &= t + a_1 \\ F_2(t) &= t^2 + a_1 t + a_2 \\ &\cdots\cdots\cdots\cdots \\ F_{n-1}(t) &= t^{n-1} + a_1 t^{n-2} + a_2 t^{n-3} + \cdots + a_{n-1}, \end{aligned}$$

so dass die Potenzen $1, t, t^2, \ldots, t^{n-1}$ ohne Nenner durch $F_0, F_1, \ldots, F_{n-1}$ dargestellt werden können, und dass jede ganze Zahl oder jedes ganze Functional ω auch den Ausdruck erhält:

$$(16) \qquad \omega = B_0 F_0(\tau) + B_1 F_1(\tau) + \cdots + B_{n-1} F_{n-1}(\tau),$$

dessen Coëfficienten $B_0, B_1, \ldots, B_{n-1}$ ganze rationale Functionale sind.

Betrachten wir jetzt die ganze Function von t:

$$S \frac{F(t)}{(t - \tau) F'(\tau)},$$

worin S das Zeichen für die in §. 134 erklärte Spur ist, so ergiebt sich, dass sie den Werth 1 erhält für $t = \tau_1, \tau_2, \ldots, \tau_n$

und dass sie also, da sie nur vom $(n-1)^{\text{ten}}$ Grade ist, identisch $= 1$ sein muss. Daraus folgt nach (14):

$$1 = t^{n-1} S \frac{F_0(\tau)}{F'(\tau)} + t^{n-2} S \frac{F_1(\tau)}{F'(\tau)} + \cdots + S \frac{F_{n-1}(\tau)}{F'(\tau)}$$

oder

$$(17) \qquad S \frac{F_\nu(\tau)}{F'(\tau)} = 0, \quad S \frac{F_{n-1}(\tau)}{F'(\tau)} = 1,$$
$$\nu = 0, 1, \ldots, n-2.$$

Hieraus ergiebt sich mit Benutzung von (16):

$$(18) \qquad S \frac{\omega}{F'(\tau)} = B_{n-1},$$

oder der Satz:

4. Ist ω eine ganze Zahl oder ein ganzes Functional des Körpers Ω, so ist die Spur von $\frac{\omega}{F'(\tau)}$ ein ganzes rationales Functional.

Neunzehnter Abschnitt.

Beziehungen eines Körpers auf seine Theiler.

---

§. 159.

Relativnormen.

Wir wollen in diesem Abschnitte die Modificationen betrachten, die in den Definitionen und Sätzen der Theorie der algebraischen Zahlen eintreten, wenn an Stelle des absoluten Rationalitätsbereiches, d. h. des Körpers der rationalen Zahlen, ein beliebiger algebraischer Zahlkörper gesetzt wird. Es werden sich dabei einige wichtige Ergänzungen auch für die allgemeine Theorie der Primfactoren ergeben, die in einer Reihe von Dedekind und Hilbert aufgestellter Sätze ihren Ausdruck finden [1]).

Es sei also R ein algebraischer Zahlkörper m^{ten} Grades und

$$(1) \qquad f(\Theta) = \Theta^n + \alpha_1 \Theta^{n-1} + \cdots + \alpha_n = 0$$

eine in R rationale und irreducible Gleichung n^{ten} Grades. Der Körper $\Omega = R(\Theta)$ ist ein algebraischer Körper über R, der in Bezug auf R vom n^{ten} Grade ist (Bd. I, §. 142). Im absoluten Rationalitätsbereiche ist Ω vom Grade $m\,n$, und wenn ϱ eine Primitivzahl des Körpers R ist, so ist

$$(2) \qquad \Theta^s \varrho^t, \quad \begin{matrix} s = 0, 1, \ldots, n-1 \\ t = 0, 1, \ldots, m-1 \end{matrix}$$

eine Basis des Körpers Ω; denn wegen der Irreducibilität der

---

[1]) Dedekind, „Ueber die Discriminanten endlicher Körper“, Abhandlungen der Göttinger Gesellschaft der Wissenschaften (1882). „Zur Theorie der Ideale“, Nachrichten der Gesellschaft der Wissenschaften zu Göttingen, 1894, Nr. 4. Hilbert, „Grundzüge einer Theorie des Galois'schen Zahlkörpers“. Ebend. 1894, Nr. 3.

Gleichung (1) kann zwischen den mn Zahlen (2) keine lineare Relation mit rationalen Zahlencoëfficienten bestehen.

Jede Zahl ω des Körpers Ω kann als ganze Function $(n-1)^{\text{ten}}$ Grades von Θ mit Coëfficienten in R dargestellt werden, und jede solche Zahl ω genügt einer in R irreduciblen Gleichung höchstens vom n^{ten} Grade; ω ist dann und nur dann eine ganze Zahl, wenn diese Gleichung, nachdem der Coëfficient der höchsten Potenz auf 1 gebracht ist, ganze Zahlen in R zu Coëfficienten hat.

Den Inbegriff aller ganzen Zahlen in Ω bezeichnen wir, wie früher, mit $\mathfrak{o}$.

Wenn wir, ohne die Zahlen des Körpers R zu verändern, für Θ die sämmtlichen Wurzeln $\Theta_1, \Theta_2, \ldots, \Theta_n$ der Gleichung (1) nehmen, so erhalten wir n Körper

(3) $$\Omega_1 = R(\Theta_1),\ \Omega_2 = R(\Theta_2), \ldots, \Omega_n = R(\Theta_n),$$

die in Bezug auf den Körper R conjugirt sind.

Sind $\omega_1, \omega_2, \ldots, \omega_n$ entsprechende Zahlen dieser Körper, so heisst das Product

(4) $$\mathfrak{N}_R(\omega) = \omega_1 \omega_2 \ldots \omega_n$$

die in Bezug auf R genommene Partialnorm (Relativnorm) der Zahl ω.

Eine Zahl η des Körpers R hat eine in diesem Körper genommene gewöhnliche Norm $N_R(\eta)$, die eine rationale Zahl ist. Die Relativnorm $\mathfrak{N}_R(\omega)$ ist nun eine solche Zahl η, und wenn wir ihre Norm im Körper R nehmen, so erhalten wir die Totalnorm der Zahl ω im Körper der rationalen Zahlen:

(5) $$N_\Omega(\omega) = N_R \mathfrak{N}_R(\omega).$$

Dies ergiebt sich, wenn man ω durch die Potenzen (2) von Θ und ϱ ausdrückt, sodann für ϱ die m conjugirten Werthe, und zu jedem dieser ϱ die nach R conjugirten Werthe Θ setzt.

In demselben Sinne haben nun auch die Functionale des Körpers Ω und die durch diese repräsentirten Ideale ihre Partialnormen. Die Partialnorm eines Functionals in Ω ist ein Functional in R, und demnach ist die Partialnorm eines Ideals in Ω ein Ideal in R.

Von den conjugirten Idealen können auch zwei oder mehrere einander gleich sein, und zwar kann dies auch dann eintreten, wenn die die Ideale repräsentirenden conjugirten Functionale nicht identisch sind, wenn sie nur associirt sind. Wenn man

daher nur das Product aller von einander verschiedenen unter den conjugirten Idealen nimmt, so braucht dies keineswegs ein Ideal in R zu sein.

Was hier von den Normen ausgeführt ist, gilt auch von den anderen symmetrischen Functionen, insbesondere von den Spuren. Wir nennen die Summe

$$(6) \qquad \mathfrak{S}_R(\omega) = \omega_1 + \omega_2 + \cdots + \omega_n$$

die Partialspur (oder Relativspur) von ω in Bezug auf R. Sie ist eine Zahl oder ein Functional in R, und wir erhalten für die Totalspur

$$(7) \qquad S_\Omega(\omega) = S_R\,\mathfrak{S}_R(\omega),$$

worin die Bedeutung der Zeichen unmittelbar verständlich ist.

Eine besonders wichtige Beziehung ergiebt sich aber durch die Betrachtung der Grundideale.

Es sei τ eine Basisform von Ω (also eine Linearform von $m\,n$ Variablen, §. 146) und

$$F(t) = N_\Omega(t - \tau)$$

die irreducible Function $m\,n^{\text{ten}}$ Grades (im absoluten Rationalitätsbereiche), deren Wurzel τ ist. Dann haben wir im §. 158 das durch das Functional $F'(\tau)$ definirte Ideal als das Grundideal des Körpers Ω bezeichnet.

Ist nun σ eine Basisform von R und

$$\psi(t) = N_R(t - \sigma),$$

so ist durch $\psi'(\sigma)$ das Grundideal des Körpers R definirt.

Aus der Function $F(t)$ spaltet sich aber im Körper R ein irreducibler Factor n^{ten} Grades ab,

$$f(t) = \mathfrak{N}_R(t - \tau),$$

der für $t = \tau$ verschwindet. Wir definiren durch $f'(\tau)$ das Partial-Grundideal von Ω in Bezug auf R, und beweisen nun den Satz:

$$(8) \qquad F'(\tau) = \varepsilon\, f'(\tau)\, \psi'(\sigma),$$

worin ε eine Einheit ist.

Um ihn zu beweisen, setzen wir nach der im §. 158 angewandten Bezeichnung

$$(9) \qquad \frac{F(t)}{t-\tau} = t^{m\,n-1} F_0(\tau) + t^{m\,n-2} F_1(\tau) + \cdots + F_{m\,n-1}(\tau),$$

$$(10) \qquad \frac{f(t)}{t-\tau} = t^{n-1} f_0(\tau) + t^{n-2} f_1(\tau) + \cdots + f_{n-1}(\tau),$$

$$(11) \qquad \frac{\psi(t)}{t-\sigma} = t^{m-1}\psi_0(\sigma) + t^{m-2}\psi_1(\sigma) + \cdots + \psi_{m-1}(\sigma).$$

Hierin sind F_ν, ψ_ν ganze Functionale des absoluten Rationalitätsbereiches, während f_ν ganze Functionale in R sind. Die Ausdrücke für F_ν, f_ν, ψ_ν ergeben sich aus den Formeln §. 158, (15). Auf diese Functionale kann man dieselben Schlüsse anwenden, die zu dem Theorem §. 158, 4. geführt haben, und es ergiebt sich:

$$(12)\qquad \begin{aligned} \mathfrak{S}_R \frac{f_\nu(\tau)}{f'(\tau)} &= 0, \\ \mathfrak{S}_R \frac{f_{n-1}(\tau)}{f'(\tau)} &= 1. \end{aligned} \qquad \nu = 0, 1, \ldots, n-2.$$

Wenn man nun die Functionen $F_\nu(t)$, wenn sie von höherem als $(n-1)^{\text{ten}}$ Grade sind, durch $f(t)$ dividirt und den Rest der Division nimmt, dann in diesem Reste die Potenzen von t [nach §. 158, (15), auf f_ν angewandt], durch die Functionen $f_\nu(t)$ ausdrückt, so ergiebt sich die Darstellung

$$(13)\qquad F_\nu(\tau) = \alpha_0 f_0 + \alpha_1 f_1 + \cdots + \alpha_{n-1} f_{n-1},$$

worin die $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ ganze Functionale in R sind. Diese Darstellung gilt für jede Wurzel τ von $f(t) = 0$, d. h. für $\tau = \tau_1, \tau_2, \ldots, \tau_n$. Hieraus ergiebt sich aber nach (12):

$$\mathfrak{S}_R \left(\frac{F_\nu(\tau)}{f'(\tau)}\right) = \alpha_{n-1}.$$

Dividirt man hier durch $\psi'(\sigma)$ und bildet die Spur S_R, so erhält man aus (7) mit Anwendung des Satzes 4., §. 158:

$$(14)\qquad S_\Omega \left(\frac{F_\nu(\tau)}{f'(\tau)\,\psi'(\sigma)}\right) = a_\nu,$$

worin a_ν ein ganzes rationales Functional bedeutet.

Nach (9) ist nun für jede Wurzel τ_i von $F(t) = 0$ mit Ausnahme von $\tau_i = \tau$

$$\tau^{nm-1} F_0(\tau_i) + \tau^{nm-2} F_1(\tau_i) + \cdots + F_{nm-1}(\tau_i) = 0,$$

und

$$\tau^{nm-1} F_0(\tau) + \tau^{nm-2} F_1(\tau) + \cdots + F_{nm-1}(\tau) = F'(\tau),$$

so dass sich, wenn man (14) mit $\tau^{nm-\nu-1}$ multiplicirt und die Summe in Bezug auf ν nimmt,

$$(15)\qquad \frac{F'(\tau)}{f'(\tau)\,\psi'(\sigma)} = a_0\,\tau^{nm-1} + a_1\,\tau^{nm-2} + \cdots$$

ergiebt. Es ist daher $F'(\tau)$ durch $f'(\tau)\,\psi'(\sigma)$ theilbar.

Andererseits ist $f_\nu(\tau)\,\psi_\mu(\sigma)$ ein ganzes Functional des Körpers Ω, und folglich nach dem vorhin schon angewandten Satze §. 158, 4.:

$$(16)\qquad S_\Omega\left(\frac{f_\nu(\tau)\,\psi_\mu(\sigma)}{F'(\tau)}\right) = b_{\mu,\nu} \qquad \begin{array}{l}\mu = 0, 1, \ldots, m-1\\ \nu = 0, 1, \ldots, n-1\end{array}$$

ein ganzes rationales Functional. Multiplicirt man diese Gleichung mit $\tau^{n-\nu-1}\,\sigma^{m-\mu-1}$ und nimmt die Summe über alle μ und ν, so folgt, wie vorhin, da für zwei von σ, τ verschiedene Wurzeln σ_k, τ_i von $\psi = 0$, $f = 0$

$$\sigma^{m-1}\,\psi_0(\sigma_k) + \sigma^{m-2}\,\psi_1(\sigma_k) + \cdots + \psi_{m-1}(\sigma_k) = 0,$$
$$\tau^{n-1}\,f_0(\tau_i) + \tau^{n-2}\,f_1(\tau_i) + \cdots + f_{n-1}(\tau_i) = 0,$$

und

$$\sigma^{m-1}\,\psi_0(\sigma) + \sigma^{m-2}\,\psi_1(\sigma) + \cdots + \psi_{m-1}(\sigma) = \psi'(\sigma),$$
$$\tau^{n-1}\,f_0(\tau) + \tau^{n-2}\,f_1(\tau) + \cdots + f_{n-1}(\tau) = f'(\tau)$$

ist, die Gleichung

$$(17)\qquad \frac{f'(\tau)\,\psi'(\sigma)}{F'(\tau)} = \sum^{\mu,\nu} b_{\mu,\nu}\,\tau^{n-\nu-1}\,\sigma^{m-\mu-1}.$$

Also ist auch $f'(\tau)\,\psi'(\sigma)$ durch $F'(\tau)$ theilbar und unser Theorem (8) daher bewiesen.

Bezeichnen wir mit G_Ω, G_R die Grundideale der Körper Ω, R, mit $\mathfrak{G}_R$ das relative Grundideal von Ω in Bezug auf R, so kann man dem bewiesenen Theorem auch den Ausdruck geben:

$$(18)\qquad G_\Omega = \mathfrak{G}_R\,G_R.$$

Es ist klar, wie sich dieses Theorem verallgemeinern lässt: Es sei

$$\Omega_1,\ \Omega_2,\ \Omega_3,\ \ldots$$

eine Reihe von Körpern, deren jeder die folgenden als Theiler enthält. Es sei ferner $\mathfrak{G}_{i,k}$ das Grundideal von Ω_i in Bezug auf Ω_k $(k > i)$, dann ist

$$(19)\qquad \mathfrak{G}_{i,k} = \mathfrak{G}_{i,i+1}\,\mathfrak{G}_{i+1,i+2}\cdots\mathfrak{G}_{k-1,k}.$$

Die tiefere Bedeutung dieser Grundideale wird sich in einem der nächsten Paragraphen noch deutlicher herausstellen.

Wir wollen aber schon hier auf eine merkwürdige Erscheinung aufmerksam machen, dass es nämlich vorkommen kann, dass $f'(\tau)$ eine Einheit ist, was nach dem Minkowski'schen Satze nicht möglich ist, wenn R der Körper der rationalen Zahlen ist. In diesen Fällen, von denen die Theorie der com-

plexen Multiplication der elliptischen Functionen Beispiele giebt, ist das Partial-Grundideal $\mathfrak{G}_R$ gleich 1 zu setzen.

Wenn die n Körper (3) mit einander identisch sind, so heisst Ω ein Normalkörper in Bezug auf R (relativ normal, wenn R nicht der absolute Rationalitätsbereich ist). Die Gesammtheit der n Substitutionen (Θ, Θ_n), die den Uebergang der Zahlen des Körpers Ω zu den conjugirten Zahlen vermitteln, bilden eine Gruppe vom Grade n, wie wir schon im §. 147 des ersten Bandes gesehen haben, die nichts anderes ist, als die Galois'sche Gruppe der Gleichung (1) im Rationalitätsbereiche R, die wir hier die Gruppe des Körpers Ω (in Bezug auf R) nennen.

Wenn insbesondere diese Gruppe commutativ ist, so ist Ω ein Abel'scher Körper in Bezug auf R (ein relativ Abel'scher Körper). In diesem Falle ist (1) eine Abel'sche Gleichung im Rationalitätsbereiche R.

§. 160.

Primideale im relativ normalen Körper.

Wir nehmen jetzt an, dass der Körper Ω normal sei in Bezug auf den beliebigen Körper R, und untersuchen unter dieser Voraussetzung die Primideale des Körpers Ω.

Die Gruppe von Ω in Bezug auf R sei Φ, und die Substitutionen von Φ mögen mit $\varphi, \varphi_1, \ldots$ bezeichnet sein. Wir bezeichnen ferner mit

(1) $$\omega \mid \varphi$$

die Zahl, die durch die Substitution φ aus ω hervorgeht, so dass ω und $\omega \mid \varphi$ in Ω enthalten sind.

Ebenso wie die Zahlen ω gehen auch alle Functionale und damit zugleich alle Ideale $\mathfrak{a}$ des Körpers Ω durch eine Substitution φ in bestimmte Functionale und Ideale $\mathfrak{a} \mid \varphi$ über, und wenn ω eine durch $\mathfrak{a}$ theilbare ganze Zahl ist, so ist $\omega \mid \varphi$ durch $\mathfrak{a} \mid \varphi$ theilbar.

Wenn $\mathfrak{a}$ irgend ein Ideal in Ω ist, so giebt es gewisse Substitutionen ψ in Φ, die der Bedingung

(2) $$\mathfrak{a} \mid \psi = \mathfrak{a}$$

genügen, darunter immer die identische Substitution, und diese Substitutionen ψ bilden eine Gruppe Ψ, die ein Theiler von Φ

ist. Wir nennen Ψ die zum Ideal $\mathfrak{a}$ gehörige Gruppe, und wir sagen auch, $\mathfrak{a}$ gehört zu der Gruppe Ψ.

Da man in jeder Gleichung zwischen Zahlen und Functionalen in Ω alle Substitutionen der Gruppe Φ ausführen darf, wobei die Grössen des Körpers R ungeändert bleiben, ohne dass die Gleichung zu bestehen aufhört, so folgt, dass Einheiten, ganze Functionale, associirte Functionale, durch einander theilbare Functionale diese Eigenschaften nicht verlieren, wenn irgend eine der Substitutionen von Φ ausgeführt wird. Wir heben den Satz hervor:

1. Ist $\mathfrak{p}$ ein Primideal, so sind auch alle mit $\mathfrak{p}$ in Bezug auf R conjugirten Ideale $\mathfrak{p}|\varphi$ Primideale. Ist $\mathfrak{a}$ durch irgend eine Potenz von $\mathfrak{p}$ theilbar so ist $\mathfrak{a}|\varphi$ durch die gleiche Potenz von $\mathfrak{p}|\varphi$, theilbar.

Ist $\mathfrak{p}$ ein Primideal in Ω, so giebt es eine und nur eine durch $\mathfrak{p}$ theilbare natürliche Primzahl p.

Zerlegt man diese in ihre Primfactoren in R, so muss einer dieser Primfactoren, den wir mit $\mathfrak{P}$ bezeichnen, durch $\mathfrak{p}$ theilbar sein.

Ist dann $\mathfrak{A}$ irgend ein Ideal in R und zugleich durch $\mathfrak{p}$ theilbar, so ist der grösste gemeinschaftliche Theiler von $\mathfrak{P}$ und $\mathfrak{A}$, der nach §. 139 auch in R enthalten ist, durch $\mathfrak{p}$ theilbar, und ist also gewiss keine Einheit. $\mathfrak{P}$ und $\mathfrak{A}$ sind also nicht relativ prim, und $\mathfrak{A}$ ist folglich durch das Primideal $\mathfrak{P}$ theilbar. Ist $\mathfrak{A}$ auch ein Primideal, so müssen $\mathfrak{A}$ und $\mathfrak{P}$ identisch sein. Damit ist, mit Rücksicht auf 1., bewiesen:

2. Ist $\mathfrak{p}$ ein Primideal in Ω, so giebt es ein und nur ein Primideal $\mathfrak{P}$ in R, das durch $\mathfrak{p}$ theilbar ist, und jedes durch $\mathfrak{p}$ theilbare Ideal in R ist zugleich durch $\mathfrak{P}$ theilbar. Das Primideal $\mathfrak{P}$ ist zugleich durch die sämmtlichen zu $\mathfrak{p}$ conjugirten Primideale $\mathfrak{p}|\varphi$ theilbar.

Die Partialnorm $\mathfrak{N}_R(\mathfrak{p})$ ist durch $\mathfrak{p}$, und folglich als Ideal in R durch $\mathfrak{P}$ theilbar. Sie kann aber auch nach dem Satze 1. durch kein von $\mathfrak{P}$ verschiedenes Ideal in R theilbar sein. Denn ist $\mathfrak{P}'$ irgend ein Primtheiler von $\mathfrak{N}_R(\mathfrak{p})$, so ist $\mathfrak{P}'$ wenigstens durch einen der Primfactoren $\mathfrak{p}|\varphi$ theilbar und mithin gleich $\mathfrak{P}$. Folglich

ist die Partialnorm von $\mathfrak{p}$ eine Potenz von $\mathfrak{P}$. Wir setzen

(3) $$\mathfrak{N}_R(\mathfrak{p}) = \mathfrak{P}^f,$$

und nennen f den Grad von $\mathfrak{p}$ in Bezug auf den Körper R.

Die Norm von $\mathfrak{P}$ im Körper R ist gleichfalls eine Potenz von p, die wir mit P bezeichnen wollen, also

(4) $$N_R(\mathfrak{P}) = P.$$

Es ergiebt sich dann für die Totalnorm von $\mathfrak{P}$ im Körper Ω nach §. 159, (5)

(5) $$N_\Omega(\mathfrak{p}) = P^f.$$

Ist $\mathfrak{p}^g$ die höchste in $\mathfrak{P}$ aufgehende Potenz von $\mathfrak{p}$, so ist $\mathfrak{P}$ nach 1. auch durch die g^{te} Potenz aller mit $\mathfrak{p}$ conjugirten Primfactoren und durch keine höhere Potenz theilbar. Wenn nun $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_e$ die von einander verschiedenen unter den mit $\mathfrak{p}$ conjugirten Primidealen sind, so ist

(6) $$\mathfrak{P} = (\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_e)^g,$$

und wenn man die Partialnorm auf beiden Seiten nimmt, und wie früher mit n den Grad des Körpers Ω in Bezug auf R bezeichnet, so dass die Partialnorm von $\mathfrak{P}$ gleich $\mathfrak{P}^n$ wird, so folgt aus (3):

(7) $$n = e f g.$$

Es sind also die natürlichen Zahlen e, f, g Theiler von n.

Wenn $\mathfrak{p}$ durch φ_1 in $\mathfrak{p}_1$ übergeht, wenn also

$$\mathfrak{p}_1 = \mathfrak{p} \,|\, \varphi_1,$$

so ist $\mathfrak{p} = \mathfrak{p}_1 \,|\, \varphi_1^{-1}$, und wenn Ψ die zu $\mathfrak{p}$ gehörige Gruppe ist, so ist auch für jede in Ψ enthaltene Substitution ψ

$$\mathfrak{p}_1 = \mathfrak{p} \,|\, \psi \varphi_1, \quad \mathfrak{p}_1 = \mathfrak{p}_1 \,|\, \varphi_1^{-1} \psi \varphi_1.$$

Ist umgekehrt $\mathfrak{p}_1 \,|\, \varphi = \mathfrak{p}_1$, so folgt $\mathfrak{p} \,|\, \varphi_1 \varphi \varphi_1^{-1} = \mathfrak{p}$, d. h. $\varphi_1 \varphi \varphi_1^{-1} = \psi$ oder $\varphi = \varphi_1^{-1} \psi \varphi_1$.

Es gehört daher $\mathfrak{p}_1$ zur Gruppe $\varphi_1^{-1} \Psi \varphi_1$, und wenn

$$\mathfrak{p}_1 = \mathfrak{p} \,|\, \varphi_1, \; \mathfrak{p}_2 = \mathfrak{p} \,|\, \varphi_2, \ldots, \mathfrak{p}_e = \mathfrak{p} \,|\, \varphi_e$$

ist, so ist

(8) $$\Phi = \Psi \varphi_1 + \Psi \varphi_2 + \cdots + \Psi \varphi_e.$$

Ψ ist also ein Theiler von Φ vom Index e und vom Grade gf.

§. 161.

Primitivwurzeln der Primideale.

Aus den Formeln (4), (5) des vorigen Paragraphen ergiebt sich, mit Rücksicht auf §. 150, für jede ganze Zahl η des Körpers R

$$\eta^P \equiv \eta \pmod{\mathfrak{P}},$$

also auch

(1) $$\eta^P \equiv \eta \pmod{\mathfrak{p}},$$

und für jede Zahl ω in $\mathfrak{o}$

(2) $$\omega^{P^f} \equiv \omega \pmod{\mathfrak{p}}.$$

Die Anzahl der nach $\mathfrak{P}$ incongruenten ganzen Zahlen in R ist P, und die Anzahl der nach $\mathfrak{p}$ incongruenten Zahlen in Ω ist P^f.

Wir haben schon früher (§. 150) gezeigt, dass es zu jedem Primideal $\mathfrak{p}$ Primitivwurzeln γ giebt, d. h. Zahlen in Ω, die der Congruenz

(3) $$\gamma^{P^f-1} \equiv 1 \pmod{\mathfrak{p}}$$

genügen, und zugleich die Eigenschaft haben, dass keine niedrigere Potenz mit positiven Exponenten der Einheit congruent wird. Dann ist jede durch $\mathfrak{p}$ nicht theilbare ganze Zahl in Ω mit einer und nur mit einer der Potenzen von γ

(4) $$1, \gamma, \gamma^2, \ldots, \gamma^{P^f-2}$$

nach dem Modul $\mathfrak{p}$ congruent.

Jede ganze Zahl Θ in Ω genügt einer Gleichung höchstens vom n^{ten} Grade, deren Coëfficienten ganze Zahlen in R sind.

Diese Gleichung ist zugleich eine Congruenz nach dem Modul $\mathfrak{p}$, und unter allen solchen Congruenzen wird es eine von möglichst niedrigem Grade

$$F(\Theta) \equiv 0 \pmod{\mathfrak{p}}$$

geben, in der wir überdies den Coëfficienten der höchsten Potenz von Θ gleich 1 annehmen können. Denn ist der höchste (durch $\mathfrak{p}$ und folglich durch $\mathfrak{P}$ untheilbare) Coëfficient η_0, so können wir immer der Congruenz

$$\eta_0\, \eta \equiv 1 \pmod{\mathfrak{P}}$$

durch ein ganzzahliges η in R genügen, und haben dann nur die Function F mit diesem η zu multipliciren. Wir können

also, wenn t eine Variable ist, die Function F in der Form annehmen:

$$F(t) = t^\nu + \alpha_1 t^{\nu-1} + \alpha_2 t^{\nu-2} + \cdots + \alpha_\nu,$$

deren Coëfficienten $\alpha_1, \alpha_2, \ldots, \alpha_\nu$ ganze Zahlen in R sind. Durch Division können wir dann für jede andere ganze Function $F_1(t)$ den Quotienten $Q(t)$ und den Rest $\varphi(t)$ so bestimmen, dass

(5) $$F_1(t) = Q(t)\, F(t) + \varphi(t),$$

worin

(6) $$\varphi(t) = \varrho_0 + \varrho_1 t + \cdots + \varrho_{\nu-1} t^{\nu-1}$$

eine durch $F_1(t)$ eindeutig bestimmte Function $(\nu - 1)^{\text{ten}}$ Grades ist, mit ganzzahligen Coëfficienten ϱ.

Setzen wir für Θ die Primitivwurzel γ und für $F_1(t)$ eine Potenz von t, so ergiebt sich aus (4), (5) und (6), dass jede durch $\mathfrak{p}$ nicht theilbare Zahl ω einer Congruenz

(7) $$\omega \equiv \varrho_0 + \varrho_1 \gamma + \cdots + \varrho_{\nu-1} \gamma^{\nu-1} \pmod{\mathfrak{p}}$$

genügt, und da die ϱ auch $= 0$ sein können, so gilt dies auch noch für ein durch $\mathfrak{p}$ theilbares ω.

Die Coëfficienten ϱ in dem Ausdrucke (7) sind durch ω selbst nach dem Modul $\mathfrak{P}$ völlig bestimmt, da nach unserer Voraussetzung γ keiner Congruenz in R von niedrigerem als dem ν^{ten} Grade genügen soll, deren Coëfficienten nicht alle durch $\mathfrak{P}$ theilbar sind. Folglich giebt es, da jeder der Coëfficienten in (7) nur P incongruente Werthe haben kann, P^ν und nicht mehr incongruente Zahlen ω, und daraus folgt, dass $\nu = f$ sein muss.

Aus einer Congruenz $F(\gamma) \equiv 0 \pmod{\mathfrak{p}}$ folgt nun aber durch wiederholtes Potenziren mit Rücksicht auf (1):

$$F(\gamma^P) \equiv 0,\ F(\gamma^{P^2}) \equiv 0, \ldots \pmod{\mathfrak{p}},$$

und wir haben also den Satz bewiesen (§. 150, 2.):

Eine Primitivwurzel γ von $\mathfrak{p}$ genügt nach dem Modul $\mathfrak{p}$ einer Congruenz in R vom f^{ten} Grade, deren sämmtliche Wurzeln

$$\gamma, \gamma^P, \gamma^{P^2}, \ldots, \gamma^{P^{f-1}}$$

sind.

Diesem Satze kann man auch den Ausdruck geben:

Das Product

(8) $$(t - \gamma)(t - \gamma^P) \ldots (t - \gamma^{P^{f-1}})$$

ist nach dem Modul $\mathfrak{p}$ mit einer ganzen Function $F(t)$ in R congruent.

§. 162.

Das Partial-Grundideal.

Es möge jetzt

(1) $$\tau = t_1 \omega_1 + t_2 \omega_2 + \cdots + t_{mn} \omega_{mn}$$

eine Basisform von $\mathfrak{o}$ sein. Dann wird es gewisse Substitutionen χ in Φ geben, und darunter immer die identische, die der Congruenz

(2) $$\tau \,|\, \chi \equiv \tau \pmod{\mathfrak{p}}$$

genügen. Alle diese Substitutionen bilden eine in Φ enthaltene Gruppe X, die auch ein Theiler der Gruppe Ψ ist, zu der $\mathfrak{p}$ gehört. Denn aus τ erhält man (nach §. 146) eine Basisform von $\mathfrak{p}$, wenn man für die Variablen t gewisse lineare Functionen neuer Variablen mit ganzen rationalen Coëfficienten setzt; wenn also π eine solche Basisform von $\mathfrak{p}$ ist, so folgt aus (2), dass $\pi \,|\, \chi$ durch π theilbar und daher auch $\mathfrak{p} \,|\, \chi = \mathfrak{p}$ ist.

Nun genügt τ einer Gleichung n^{ten} Grades $f(t) = 0$, deren Coëfficienten ganze Functionen in R mit den Variablen $t_1, t_2 \ldots$ sind, und es ist, wenn t eine neue Variable bedeutet, und $\tau_1, \tau_2, \ldots, \tau_n$ die in Bezug auf R zu τ conjugirten Formen sind,

(3) $$f(t, t_1, t_2, \ldots) = f(t) = (t - \tau_1)(t - \tau_2) \ldots (t - \tau_n).$$

Hieraus ergiebt sich nun, wenn wir wiederholt in die Potenz p erheben, und auf die Zahlencoëfficienten von f die Formel §. 161, (1) anwenden:

(4) $$f(t^P, t_1^P, t_2^P, \ldots) \equiv [f(t)]^P$$
$$\equiv (t^P - \tau_1')(t^P - \tau_2') \ldots (t^P - \tau_n') \pmod{\mathfrak{p}},$$

wenn $\tau_1', \tau_2', \ldots, \tau_n'$ dadurch aus $\tau_1, \tau_2, \ldots, \tau_n$ abgeleitet sind, dass die Variablen $t_1, t_2, \ldots$ durch $t_1^P, t_2^P, \ldots$ ersetzt sind.

Setzen wir nun $t = \tau$ in (4), so verschwindet $f(t)$ und es folgt, dass einer der Factoren des letzten Productes durch $\mathfrak{p}$ theilbar sein muss. Dies aber kann so ausgedrückt werden, dass es in Φ eine Substitution ψ_0 giebt, die der Bedingung

(5) $$\tau^P \equiv \tau' \,|\, \psi_0 \pmod{\mathfrak{p}}$$

genügt.

Aus τ entstehen alle ganzen Zahlen in Ω, wenn man für die Variablen ganze rationale Zahlen setzt. Wendet man dann

noch den Fermat'schen Lehrsatz für rationale Zahlen an, so erkennt man, dass die Congruenzen (2) und (5) gleichbedeutend sind mit den für jede Zahl ω in $\mathfrak{o}$ gültigen Formeln

(6) $$\omega \,|\, \chi \equiv \omega, \ \omega^P \equiv \omega \,|\, \psi_0 \pmod{\mathfrak{p}}.$$

Aus der zweiten Congruenz (6) folgt, dass, wenn ω durch $\mathfrak{p}$ theilbar ist, immer auch $\omega \,|\, \psi_0$ durch $\mathfrak{p}$ theilbar sein muss. Folglich ist $\mathfrak{p}$ durch $\mathfrak{p} \,|\, \psi_0$ theilbar, und als Primideal $= \mathfrak{p} \,|\, \psi_0$. Daraus folgt, dass ψ_0 in der Gruppe Ψ enthalten ist.

Wir verstehen jetzt unter γ eine Primitivwurzel von $\mathfrak{p}$ und wenden die am Schlusse des §. 161 bewiesene Formel an:

(7) $$(t-\gamma)(t-\gamma^P)\ldots(t-\gamma^{P^{f-1}}) \equiv F(t) \pmod{\mathfrak{p}},$$

in der $F(t)$ eine ganze Function von t in R ist.

Daraus folgt

$$F(\gamma) \equiv 0 \pmod{\mathfrak{p}},$$

und wenn nun ψ irgend eine Substitution aus Ψ ist:

$$F(\gamma \,|\, \psi) \equiv 0 \pmod{\mathfrak{p}}.$$

Daraus ergiebt sich aber, dass $\gamma \,|\, \psi$ mit einer der in (7) vorkommenden Potenzen von γ nach $\mathfrak{p}$ congruent sein muss, also etwa

(8) $$\gamma^{P^\nu} \equiv \gamma \,|\, \psi \pmod{\mathfrak{p}}.$$

Nun ist jede durch $\mathfrak{p}$ nicht theilbare Zahl ω in $\mathfrak{o}$ mit einer Potenz von γ congruent, und wenn man also (8) zu dieser Potenz erhebt, so folgt

(9) $$\omega^{P^\nu} \equiv \omega \,|\, \psi \pmod{\mathfrak{p}},$$

und diese Congruenz gilt offenbar auch noch, wenn ω durch $\mathfrak{p}$ theilbar ist, also für alle Zahlen in $\mathfrak{o}$.

Wenn wir nun die zweite der Congruenzen (6) ν mal nach einander anwenden, so folgt

(10) $$\omega^{P^\nu} \equiv \omega \,|\, \psi_0^\nu \pmod{\mathfrak{p}},$$

also

(11) $$\omega \,|\, \psi \equiv \omega \,|\, \psi_0^\nu \pmod{\mathfrak{p}},$$

und wenn wir ω durch $\omega \,|\, \psi^{-1}$ ersetzen oder auf (11) die Substitution ψ^{-1} anwenden:

(12) $$\omega \equiv \omega \,|\, \psi^{-1}\psi_0^\nu \equiv \omega \,|\, \psi_0^\nu \psi^{-1} \pmod{\mathfrak{p}}.$$

Es sind also sowohl $\psi^{-1}\psi_0^\nu$ als auch $\psi_0^\nu\psi^{-1}$ in X enthalten,

voraus sich ergiebt, dass jede Substitution ψ aus Ψ in einem .er Systeme (Nebengruppen)

$$X,\ X\psi_0,\ X\psi_0^2,\ \ldots$$

nthalten ist.

Wenn $\mathfrak{p}$ vom Grade f (in Bezug auf R) ist, so ist

$$\omega^{P^f} \equiv \omega \pmod{\mathfrak{p}},$$

nd P^f ist die niedrigste Potenz von P mit positiven Exponenten, die dieser Congruenz für alle ω genügt.

Setzt man also $\nu = f$ in (10), so folgt, dass ψ_0^f in X entalten ist, dass aber keine Potenz von ψ_0 mit niedrigerem positiven Exponenten diese Eigenschaft hat. Die Nebengruppen

$$X,\ X\psi_0,\ X\psi_0^2,\ \ldots,\ X\psi_0^{f-1}$$

ind also alle von einander verschieden, und es ergiebt sich:

13) $$\Psi = X + X\psi_0 + X\psi_0^2 + \cdots + X\psi_0^{f-1}.$$

Nach (12) ist aber die Gesammtheit der Substitutionen $\psi_0^\nu X$ nit $X\psi_0^\nu$ identisch (für jedes ν), also

14) $$\psi_0^\nu X = X\psi_0^\nu,$$

oraus folgt, dass X ein Normaltheiler von Ψ ist.

Da, wie wir oben gesehen haben, Ψ vom Grade gf st, so ist X vom Grade g.

In der Gruppe X giebt es nun solche Substitutionen χ_1, arunter immer die identische, für die die Congruenz

15) $$\tau \,|\, \chi_1 \equiv \tau \pmod{\mathfrak{p}^2}$$

rfüllt ist, und diese bilden eine Gruppe $X^{(1)}$, deren Grad mit g_1 ezeichnet sein mag.

Es ist zu beweisen, dass g_1 eine Potenz von p ist. ezeichnen wir nämlich mit π ein durch $\mathfrak{p}$ theilbares Primınctional, mit α ein ganzes Functional, so folgt aus (15):

16) $$\tau \,|\, \chi_1 = \tau + \pi^2\alpha,$$

nd da ebenso nach (15)

$$\alpha \,|\, \chi_1 \equiv \alpha \pmod{\mathfrak{p}^2},\quad (\pi \,|\, \chi_1)^2 \equiv \pi^2 \pmod{\mathfrak{p}^3}$$

st, so ergiebt sich aus (16)

$$\tau \,|\, \chi_1^2 \equiv \tau + 2\pi^2\alpha \pmod{\mathfrak{p}^3},$$

ınd allgemein für jeden positiven Exponenten h

$$\tau \,|\, \chi_1^h \equiv \tau + h\pi^2\alpha \pmod{\mathfrak{p}^3}.$$

Setzt man $h = p$, so ergiebt sich hieraus

$$\tau \,|\, \chi_1^p \equiv \tau \pmod{\mathfrak{p}^3},$$

und auf die gleiche Weise schliesst man hieraus für jeden Exponenten ν

(17) $$\tau \,|\, \chi_1^{p^\nu} \equiv \tau \pmod{\mathfrak{p}^{\nu+2}}.$$

Um diese Formel allgemein zu beweisen, wendet man die vollständige Induction an. Man nimmt (17) als bewiesen an und setzt

$$\tau \,|\, \chi_1^{p^\nu} = \tau + \pi^{\nu+2}\alpha;$$

daraus durch wiederholte Anwendung

$$\begin{aligned} \tau \,|\, \chi_1^{2p^\nu} &\equiv \tau + 2\pi^{\nu+2}\alpha \\ \tau \,|\, \chi_1^{3p^\nu} &\equiv \tau + 3\pi^{\nu+2}\alpha \pmod{\mathfrak{p}^{\nu+3}} \\ &\cdots\cdots\cdots \\ \tau \,|\, \chi_1^{p^{\nu+1}} &\equiv \tau + p\pi^{\nu+2}\alpha, \end{aligned}$$

also die Formel (17) für $\nu + 1$.

Nun kann man ν immer so gross annehmen, dass von den Differenzen

$$\tau - \tau_1,\ \tau - \tau_2,\ \tau - \tau_3, \ldots,$$

wenn τ von $\tau_1, \tau_2, \tau_3, \ldots$ verschieden ist, keine durch $\mathfrak{p}^{\nu-2}$ theilbar ist, und dann folgt aus (17), dass $\chi_1^{p^\nu}$ die identische Substitution sein muss. Es ist hiernach der Grad eines jeden Elementes χ_1 eine Potenz von p, und folglich kann nach dem Cauchy-Sylow'schen Satze (§. 29, I.) im Grade von $X^{(1)}$ keine von p verschiedene Primzahl aufgehen, wie bewiesen werden sollte.

Wenn also g nicht durch p theilbar ist, dann ist sicher $X^{(1)}$ die Einheitsgruppe.

Man kann auf diese Weise fortfahren und eine Gruppe $X^{(2)}$ vom Grade g_2 bilden aus der Congruenz

$$\tau \,|\, \chi_2 \equiv \tau \pmod{\mathfrak{p}^3},$$

$X^{(2)}$ ist ein Theiler von $X^{(1)}$, also g_2 gleichfalls eine Potenz von p, und so muss man schliesslich zur Einheitsgruppe gelangen. Unter den auf einander folgenden Gruppen $X^{(1)}, X^{(2)}, \ldots$ können unter Umständen auch mehrere einander gleich sein [1]).

[1]) Hilbert nennt Ψ die Zerlegungsgruppe, X die Trägheitsgruppe, $X^{(1)}$ die Verzweigungsgruppe des Ideals $\mathfrak{p}$. In der oben erwähnten Abhandlung ist noch bewiesen, dass g_1 die höchste in g aufgehende Potenz von p ist, dass $X^{(1)}$ ein Normaltheiler von X ist, und dass die ganze Gruppe Ψ metacyklisch ist.

Hiernach lässt sich die höchste Potenz des Primideals $\mathfrak{p}$ angeben, die in dem Partialgrundideal $\mathfrak{G}_R$ aufgeht. Nach §. 159 nämlich ist dies Ideal definirt durch das Product

$$f'(\tau) = (\tau - \tau_1)(\tau - \tau_2) \dots (\tau - \tau_{n-1}),$$

worin $\tau_1, \tau_2, \dots, \tau_{n-1}$ die von τ verschiedenen unter den mit τ conjugirten Functionalen sind. Einer der Factoren dieses Productes, $\tau - \tau \,|\, \varphi$, ist dann und nur dann durch $\mathfrak{p}$ theilbar, wenn φ zu X gehört. Da nun die identische Substitution ausgeschlossen ist, so folgt, dass $\mathfrak{G}$ den Factor $\mathfrak{p}$ mindestens $g - 1$ mal enthält.

Es ist aber $\tau - \tau \,|\, \chi$ dann und nur dann durch $\mathfrak{p}^2$ theilbar, wenn χ zu $X^{(1)}$ gehört, und folglich ist $\mathfrak{G}$ durch $\mathfrak{p}^{g-1+g_1-1}$ theilbar. Wir können so fortfahren und finden die genaue Potenz von $\mathfrak{p}$, die in $\mathfrak{G}$ enthalten ist. Sie hat den Exponenten

$$(g-1) + (g_1 - 1) + (g_2 - 1) + \cdots$$

Jede der Zahlen $g, g_1, g_2, \dots$ ist Theiler der vorangehenden, und $g_1, g_2, \dots$ sind Potenzen von p, und die Reihe setzt sich so lange fort, bis eine der Zahlen $g = 1$ geworden ist. Die Zusammensetzung des Grundideals $\mathfrak{G}$ ist also vollkommen durch die Zerlegung der Gruppe X bestimmt.

Die Zahlen $g, g_1, g_2, \dots$ sind überdies für alle conjugirten Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_e$ dieselben, und es folgt also

$$\mathfrak{G} = \Pi (\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e)^{g-1+g_1-1+g_2-2\dots},$$

wo sich das Productzeichen auf die Primfactoren aller Primzahlen p des Körpers Ω bezieht. Es brauchen dabei aber selbstverständlich nur die in endlicher Anzahl vorhandenen Primzahlen p berücksichtigt zu werden, für die $g > 1$ ist.

Die Partialnorm des Ideals $\mathfrak{G}$

$$\mathfrak{D} = \mathfrak{N}_R(\mathfrak{G}) = \Pi\, \mathfrak{P}^{ef(g-1+g_1-1+g_2-1+\cdots)}$$

heisst die Partial-Discriminante des Körpers Ω in Bezug auf den Körper R. Sie ist ein im Körper R gelegenes Ideal, die für den Fall, dass R der Körper der rationalen Zahlen ist, von einem Einheitsfactor abgesehen, in die Grundzahl des Körpers Ω übergeht (§. 158).

§. 163.

Die Ideale in den Theilern des Körpers Ω.

Wenn die Gruppe Φ des Körpers Ω einen Theiler Φ' hat, so gehört zu Φ' ein Körper Ω', der ein Theiler von Ω ist und

seinerseits R als Theiler enthält. Die Zahlen von Ω' bleiben durch die Substitutionen Φ' ungeändert, und Φ' ist die Gruppe des Körpers Ω in Bezug auf Ω' (vergl. Bd. I, §. 155). Wir bezeichnen den Grad von Φ', der ein Theiler von n ist, mit n' und setzen

(1) $$n = m' n'.$$

Es ist dann n' der Grad von Ω in Bezug auf Ω', und m' der Grad von Ω' in Bezug auf R.

Es ist dabei zu beachten, dass zwar Ω ein Normalkörper auch in Bezug auf Ω' ist, dass aber Ω' im Allgemeinen kein Normalkörper in Bezug auf R sein wird.

Die Primideale im Körper Ω' lassen sich nun vollständig aus denen von Ω ableiten.

Wenn $\mathfrak{p}$ irgend ein Primideal in Ω ist, so giebt es ein und nur ein durch $\mathfrak{p}$ theilbares Ideal $\mathfrak{p}'$ in Ω', und $\mathfrak{p}'$ kann als Theiler von $\mathfrak{P}$ durch keine anderen als die mit $\mathfrak{p}$ conjugirten Ideale theilbar sein. Durchläuft φ' die Substitutionen von Φ', so ist $\mathfrak{p}'$, da es durch φ' ungeändert bleibt, auch durch $\mathfrak{p} | \varphi'$ theilbar.

Wenn also $\mathfrak{p}_1'$ durch $\mathfrak{p} | \varphi_1$ theilbar ist, so ist es auch durch $\mathfrak{p} | \psi \varphi_1 \varphi'$ theilbar, wenn ψ ein beliebiges Element der Gruppe Ψ (§. 162) bedeutet.

Wenn daher φ irgend ein Element des Systemes

$$\Phi_1 = \Psi \varphi_1 \Phi'$$

ist, so ist $\mathfrak{p}_1'$ durch $\mathfrak{p} | \varphi$ theilbar. Es kommt demnach jetzt die Gruppenzerlegung in Betracht, die wir im §. 28 dieses Bandes auseinandergesetzt haben.

Wenn φ_2 ein nicht in Φ_1 enthaltenes Element aus Φ ist, so hat das System

$$\Phi_2 = \Psi \varphi_2 \Phi'$$

mit Φ_1 gar kein Element gemein. Giebt es noch ein Element φ_3, das weder in Φ_1 noch in Φ_2 vorkommt, so bildet man ebenso

$$\Phi_3 = \Psi \varphi_3 \Phi',$$

und fährt so fort, bis die ganze Gruppe Φ erschöpft ist. Man erhält so die Zerlegung

(2) $$\Phi = \Phi_1 + \Phi_2 + \Phi_3 + \cdots + \Phi_{e'}.$$

Den Grad eines dieser Systeme Φ_r können wir nach §. 28 bestimmen. Er ist gleich dem Producte des Grades von Φ multiplicirt mit dem Index des Durchschnittes Ψ_r' von Φ' mit $\Psi_r = \varphi_r^{-1} \Psi \varphi_r$ in Bezug auf Φ', oder was dasselbe ist, gleich dem Producte der Grade von Ψ und Φ', getheilt durch den

Grad h_r des Durchschnittes von Φ' und Ψ_r. Der Grad von Φ_r ist also gleich $f g n' : h_r$.

Wenn wir jetzt mit φ_r alle Elemente von Φ_r bezeichnen, so führen alle Primideale $\mathfrak{p} | \varphi_r$ in Ω zu demselben Primideale $\mathfrak{p}_r'$ in Ω'. Es ist aber noch zu zeigen, dass zwei verschiedene dieser Systeme Φ_1, Φ_2 zu verschiedenen Primidealen $\mathfrak{p}_1'$, $\mathfrak{p}_2'$ führen.

Zunächst ist ersichtlich, dass die sämmtlichen $\mathfrak{p} | \varphi_2$ von den $\mathfrak{p} | \varphi_1$ verschieden sind. Denn wenn $\mathfrak{p} | \varphi_1 = \mathfrak{p} | \varphi_2$ ist, so ist auch $\mathfrak{p} = \mathfrak{p} | \varphi_2 \varphi_1^{-1}$, also $\varphi_2 \varphi_1^{-1}$ in Ψ und folglich φ_2 in $\Psi \varphi_1$, d. h. in Φ_1 enthalten, gegen die Voraussetzung. Wir können also eine ganze Zahl α in Ω annehmen, die durch $\mathfrak{p} | \varphi_1$, aber durch keines der Ideale $\mathfrak{p} | \varphi_2$ theilbar ist. Dann ist auch keine der Zahlen $\alpha | \varphi'$ durch $\mathfrak{p} | \varphi_2$ theilbar, weil sonst $\mathfrak{p} | \varphi_1 \varphi' = \mathfrak{p} | \varphi_2$, also gegen die Voraussetzung φ_2 in Φ_1 enthalten wäre. Das Product α' aller von einander verschiedener $\alpha | \varphi'$, welches eine in Ω' enthaltene Zahl ist, ist zwar durch $\mathfrak{p}_1'$, nicht aber durch $\mathfrak{p}_2'$ theilbar. Folglich ist $\mathfrak{p}_1'$ von $\mathfrak{p}_2'$ verschieden, und es ergiebt sich also, dass e' und nicht mehr verschiedene Primideale $\mathfrak{p}'$ in $\mathfrak{P}$ aufgehen. Wir setzen daher

(3) $$\mathfrak{P} = \mathfrak{p}_1'^{a_1} \mathfrak{p}_2'^{a_2} \dots \mathfrak{p}_{e'}'^{a_{e'}},$$

worin die Exponenten $a_1, a_2, \dots, a_{e'}$ noch näher zu bestimmende natürliche Zahlen sind.

Um nun die Primideale $\mathfrak{p}_r'$ im Körper Ω zu zerlegen, können wir die Resultate der §. 160, 162 benutzen, indem wir einfach Ω' an Stelle von R treten lassen. Bedeutet dann X_r' den Durchschnitt von Φ' mit $X_r = \varphi_r^{-1} X \varphi_r$, so ist X_r der Inbegriff aller Substitutionen des Körpers Φ', die der Bedingung

$$\tau | \chi_r' \equiv \tau \pmod{\mathfrak{p}_r}$$

genügen. Bezeichnen wir daher den Grad von X_r' mit g_r, so ist $\mathfrak{p}_r'$ durch $\mathfrak{p}_r^{g_r}$, aber durch keine höhere Potenz von $\mathfrak{p}_r$ theilbar.

Der Durchschnitt Ψ_r' von Ψ_r mit Φ', dessen Grad wir schon oben mit h_r bezeichnet haben, ist der Inbegriff aller Substitutionen ψ_r' in Φ', die der Bedingung

$$\mathfrak{p}_r | \psi_r' = \mathfrak{p}_r$$

genügen, und wenn wir daher Φ' in die Nebengruppen

(4) $$\Phi' = \Psi_r' \varphi_{r,1}' + \Psi_r' \varphi_{r,2}' + \cdots + \Psi_r' \varphi_{r,e_r}$$

zerlegen, so ist

(5) $$n' = e_r h_r.$$

Wenn nun

$$\mathfrak{p}_{r,s} = \mathfrak{p}_r \mid \varphi_{r,s}$$

gesetzt wird, so ist nach §. 160, (6)

(6) $$\mathfrak{p}'_r = (\mathfrak{p}_{r,1}\,\mathfrak{p}_{r,2} \ldots \mathfrak{p}_{r,e_r})^{g_r},$$

und die Substitution von (6) in (3) ergiebt durch Vergleichung mit §. 160, (6)

(7) $$g = a_r\,g_r, \quad e_1 + e_2 + \cdots + e_{e'} = e,$$

wodurch die Exponenten a_r definirt sind.

Die in Bezug auf den Körper Ω' genommene Partialnorm von $\mathfrak{p}_{r,s}$ ist nach §. 160, (3), (7):

(8) $$\mathfrak{N}_{\Omega'}(\mathfrak{p}_{r,s}) = \mathfrak{p}_r'^{f_r},$$

wenn f_r durch die Gleichung

(9) $$n' = e_r\,f_r\,g_r, \quad (h_r = f_r\,g_r)$$

definirt wird.

Wir wollen nun die Gruppe Φ nach Φ' in Nebengruppen zerlegen, und setzen, wenn $\vartheta_1, \vartheta_2, \ldots, \vartheta_{m'}$ passend ausgewählte Substitutionen aus Φ sind:

(10) $$\Phi = \Phi'\vartheta_1 + \Phi'\vartheta_2 + \cdots + \Phi'\vartheta_{m'},$$

so dass durch die Substitutionen $\vartheta_1, \vartheta_2, \ldots, \vartheta_{m'}$ der Körper Ω' in m' conjugirte (gleiche oder verschiedene) Körper

$$\Omega'_1, \Omega'_2, \ldots, \Omega'_{m'}$$

übergeht. Der Körper Ω'_t gehört dann zu der Gruppe $\vartheta_t^{-1}\Phi'\vartheta_t$.

Wenn nun durch ϑ_t die Ideale $\mathfrak{p}'_r$ und $\mathfrak{p}_{r,s}$ in $\mathfrak{p}'_{r,t}$ und $\mathfrak{p}_{r,s,t}$ übergehen, so ist nach §. 160, (6)

(11) $$\mathfrak{p}'_{r,t} = (\mathfrak{p}_{r,1,t}\,\mathfrak{p}_{r,2,t} \ldots \mathfrak{p}_{r,e_r,t})^{g_r},$$

und das Product aller dieser Ideale für $t = 1, 2, \ldots, m'$ ist die im Körper Ω' genommene Partialnorm von $\mathfrak{p}'_r$ in Bezug auf den Körper R, die wir mit $\mathfrak{N}'_R(\mathfrak{p}'_r)$ bezeichnen. Sie muss eine Potenz von $\mathfrak{P}$ sein, und wir setzen

(12) $$\mathfrak{N}'_R(\mathfrak{p}'_r) = \mathfrak{P}^{f'_r}.$$

Um f'_r zu finden, brauchen wir nur $\mathfrak{P}$ in (12) nach §. 160, (6) in seine Primfactoren $\mathfrak{p}$ zu zerlegen, wodurch sich $e\,g\,f'_r$ Primfactoren $\mathfrak{p}$ in $\mathfrak{P}^{f'_r}$ ergeben. Bilden wir andererseits das Product der m' Factoren (11), so erhalten wir $g_r\,e_r\,m'$ solcher Primfactoren. Es ist daher

$$e\,g\,f'_r = m'\,g_r\,e_r,$$

also nach (1), (9) und §. 160, (7):

(13) $$f = f_r\,f'_r.$$

Zwanzigster Abschnitt.

Quadratische Körper.

§. 164.

Basis eines quadratischen Körpers.

Wir wollen die Resultate der allgemeinen Theorie der algebraischen Zahlen auf den besonderen Fall der Körper vom 2ten Grade, die auch quadratische Körper heissen, anwenden. Ein quadratischer Körper Ω entspringt aus einer ganzzahligen quadratischen Gleichung, und wird also aus dem Körper der rationalen Zahlen durch Adjunction einer Quadratwurzel $\sqrt{d}$ abgeleitet. Hierin kann d als positive oder negative ganze Zahl ohne quadratischen Theiler angenommen werden, und der einzige Werth $d = 1$ ist auszunehmen. Je nachdem d positiv oder negativ ist, erhalten wir einen reellen oder imaginären quadratischen Körper.

Den conjugirten Körper erhalten wir, wenn wir in allen Zahlen in Ω $\sqrt{d}$ in $-\sqrt{d}$ verwandeln. Dadurch bekommen wir aber keinen neuen Körper. Der quadratische Körper ist also ein (absoluter) Normalkörper (§. 160).

Die Zahlen des Körpers Ω sind keine anderen als die in §. 122 des ersten Bandes definirten quadratischen Irrationalzahlen, die alle in der Form $x + y\sqrt{d}$ enthalten sind, worin x und y ganze oder gebrochene rationale Zahlen bedeuten. Jede irrationale Zahl ω dieses Körpers genügt einer quadratischen Gleichung

(1) $$c\,\omega^2 = a + b\,\omega,$$

in der a, b, c ganze rationale Zahlen ohne gemeinsamen Theiler sind, von denen c als positiv angenommen werden kann, und die Verbindung

(2) $$D = b^2 + 4\,a\,c$$

haben wir die Discriminante der Zahl ω genannt. Das Verhältniss $D : d$ ist eine ganze rationale Quadratzahl. Die beiden Wurzeln von (1) erhalten den Ausdruck

(3) $$\omega = \frac{b + \sqrt{D}}{2c}, \quad \omega' = \frac{b - \sqrt{D}}{2c}.$$

Setzen wir

(4) $$D = e^2 d,$$

so wird

(5) $$\omega = \frac{b + e\sqrt{d}}{2c}, \quad \omega' = \frac{b - e\sqrt{d}}{2c},$$

und wegen (1) sind dies dann und nur dann ganze Zahlen, wenn $c = 1$ ist.

Nun ist $D \equiv 0$ oder $\equiv 1 \pmod 4$, und wenn also D gerade ist, so ist es durch 4 theilbar; b ist in diesem Falle gerade, und weil d nicht durch 4 theilbar sein kann, so muss auch e gerade sein.

Ist aber D ungerade, so sind auch b und e ungerade. Dieser Fall kann aber, wie (4) zeigt, nur dann eintreten, wenn $d \equiv 1 \pmod 4$ ist.

Daraus erhalten wir folgendes Resultat:

1. Ist $d \equiv 2$ oder $\equiv 3 \pmod 4$, so ist die Zahl
$$\omega = x + y\sqrt{d}$$
dann und nur dann eine ganze Zahl, wenn die rationalen Zahlen x, y ganze Zahlen sind. (Quadratische Irrationalzahlen erster Art, nach Dirichlet.)

2. Ist $d \equiv 1 \pmod 4$, so ist
$$\omega = \frac{x + y\sqrt{d}}{2}$$
dann und nur dann eine ganze Zahl, wenn die rationalen Zahlen x, y entweder zwei gerade oder zwei ungerade ganze Zahlen sind. (Quadratische Irrationalzahlen erster oder zweiter Art, je nachdem e gerade oder ungerade ist.)

Letzteres können wir auch so ausdrücken:

3. Ist $d \equiv 1 \pmod 4$, so ist
$$\omega = x + y\,\frac{1 + \sqrt{d}}{2}$$
dann und nur dann eine ganze Zahl, wenn die rationalen Zahlen x und y ganze Zahlen sind.

Daraus ergiebt sich eine Basis von $\mathfrak{o}$:

a) $1, \sqrt{d}, \quad d \equiv 2$ oder $\equiv 3 \pmod 4$,

b) $1, \frac{1+\sqrt{d}}{2}, \quad d \equiv 1 \pmod 4$.

Wenn wir also

$$(6) \quad \begin{array}{ll} \text{a)} \ \Theta = \sqrt{d}, & d \equiv 2, 3 \pmod 4 \\ \text{b)} \ \Theta = \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod 4 \end{array}$$

setzen, so ist $1, \Theta$ eine Basis von $\mathfrak{o}$.

Für die Grundzahl erhalten wir demnach, wenn Θ' mit Θ conjugirt ist,

$$\Delta = \begin{vmatrix} 1, \Theta \\ 1, \Theta' \end{vmatrix}^2 = (\Theta' - \Theta)^2,$$

also

$$(7) \quad \begin{array}{ll} \text{a)} \ \Delta = 4d, & d \equiv 2, 3 \pmod 4 \\ \text{b)} \ \Delta = d, & d \equiv 1 \pmod 4, \end{array}$$

$$(8) \qquad \Theta - \Theta' = \sqrt{\Delta}.$$

Die Grundzahl ist also $\equiv 0$ oder $\equiv 1 \pmod 4$, und muss, wenn sie durch 4 theilbar ist, $\equiv 8, 12 \pmod{16}$ sein [1]). Sie kann daher (in Uebereinstimmung mit dem Satze von Minkowski) weder $= \pm 1$ noch $= \pm 2$ sein. Die Grundzahl vom absolut kleinsten Werthe ist $\Delta = -3$.

§. 165.

Die Primideale in Ω.

Es bedeute nun φ ein beliebiges ganzes Functional in Ω. Wir wollen nach §. 146 eine Basis α_1, α_2 für φ, und damit die

---

[1]) Eine ganze rationale Zahl Δ, die nach dem Modul 4 mit 0 oder mit 1 congruent ist, hat Kronecker eine Zahl von Discriminantenform genannt. Hat Δ die Eigenschaft, dass sich kein quadratischer Factor so daraus absondern lässt, dass eine Zahl von Discriminantenform übrig bleibt, so heisst Δ eine Stammdiscriminante. Die Grundzahl eines quadratischen Körpers ist also immer eine Stammdiscriminante, und umgekehrt ist auch jede Stammdiscriminante Grundzahl eines quadratischen Körpers. Vergl. H. Weber, Zahlentheoretische Untersuchungen aus dem Gebiete der elliptischen Functionen. I, II, III. Nachrichten der Gesellschaft der Wissenschaften zu Göttingen. 1893.

entsprechende Basisform $\alpha_1 t_1 + \alpha_2 t_2$, die mit φ associirt ist, bestimmen. Wir haben nach §. 146, (3), wenn ω_1, ω_2 eine Basis von $\mathfrak{o}$ ist, die ganzen Zahlen $a_{1,1}, a_{1,2}, a_{2,2}$ so zu bestimmen, dass $a_{1,1}, a_{2,2}$ positiv und möglichst klein sind, und dass

$$\alpha_1 = a_{1,1}\,\omega_1, \quad \alpha_2 = a_{1,2}\,\omega_1 + a_{2,2}\,\omega_2$$

durch φ theilbar werden. Setzen wir also $(\omega_1, \omega_2) = (1, \Theta)$, so wird

(1) $$\alpha_1 = a_{1,1}, \quad \alpha_2 = a_{1,2} + a_{2,2}\,\Theta.$$

Es ist also $a_{1,1}$ die kleinste positive durch φ theilbare rationale Zahl, und $a_{2,2}$ ist die kleinste positive Zahl, für die $a_{2,2}\,\Theta$ nach dem Modul φ mit einer rationalen Zahl congruent wird.

Wir wollen dies auf den Fall anwenden, dass φ ein Primfunctional π ist. Ein solches kann hier nur vom ersten oder vom zweiten Grade sein, je nachdem seine absolute Norm gleich p oder $= p^2$ ist. Wir unterscheiden also die beiden Fälle:

$$1) \quad N_a(\pi) = p$$

oder

$$2) \quad N_a(\pi) = p^2.$$

Da hier $N(p) = p^2$ ist, so ist im ersten Falle p in zwei Primfactoren zerlegbar, im zweiten Falle enthält p nur einen Primfactor, d. h. p ist im Körper Ω selbst noch als Primzahl zu betrachten.

Bestimmen wir nun für $\varphi = \pi$ die Basis (1), so ergiebt sich zunächst $a_{1,1} = p$, und $a_{2,2}$ ist die kleinste positive ganze rationale Zahl, für die das Product $a_{2,2}\,\Theta$ modulo π mit einer rationalen Zahl congruent wird. Dafür ist aber nach §. 150, 3 die nothwendige und hinreichende Bedingung

$$(a_{2,2}\,\Theta)^p \equiv a_{2,2}\,\Theta \pmod{\pi},$$

oder, da nach dem Fermat'schen Satze $a_{2,2}^p \equiv a_{2,2}$ ist,

(2) $$a_{2,2}(\Theta^p - \Theta) \equiv 0 \pmod{\pi}.$$

Es ist also entweder $\Theta^p - \Theta \equiv 0$, und dann ist $a_{2,2} = 1$, oder $\Theta^p - \Theta$ nicht $\equiv 0$, und dann ist $a_{2,2} = p$.

Im ersten Falle ist Θ und damit jede Zahl ω mit einer rationalen Zahl congruent. Es giebt also nicht mehr als p nach dem Modul π incongruente Zahlen, und folglich ist (§. 148, 3.) $p^f = p$, $f = 1$, d. h. p in zwei Primfactoren ersten Grades zerlegbar.

Umgekehrt bilden in diesem Falle 1) die p rationalen Zahlen $0, 1, 2, \ldots, p-1$ ein volles Restsystem nach dem Modul π, und es ist folglich jede Zahl in $\mathfrak{o}$ und mithin auch Θ mit einer rationalen Zahl congruent. Also haben wir

$$\begin{array}{lll} 1) & N_a(\pi) = p & a_{2,2} = 1 \\ 2) & N_a(\pi) = p^2 & a_{2,2} = p. \end{array}$$

Im ersten Falle ist $a_{1,2}$ aus der Bedingung

$$(3) \qquad a_{1,2} + \Theta \equiv 0 \pmod{\pi}$$

zu bestimmen, im zweiten kann $a_{1,2} = 0$ genommen werden. Die Basisform von π ergiebt sich also, wenn u, v die Variablen sind,

$$\begin{array}{ll} 1) & \pi = pu + (a_{1,2} + \Theta)\, v \\ 2) & \pi = p\,(u + \Theta v), \end{array}$$

woraus man sieht, dass π im Falle 2), wie zu erwarten war, ein Hauptfunctional ist.

Um im Falle 1) die Zahl $a_{1,2}$ zu bestimmen, bilden wir die Norm von $a_{1,2} + \Theta$, die durch p theilbar sein muss. Wenn Θ durch Aenderung des Vorzeichens von $\sqrt{d}$ in Θ' übergeht, so ist nach §. 164, (8) $\Theta - \Theta' = \sqrt{\Delta}$, und für die Norm von $a_{1,2} + \Theta$ ergiebt sich nach §. 164 (6), a), b):

$$(4) \qquad \begin{aligned} N(a_{1,2} + \Theta) &= (a_{1,2} + \Theta)(a_{1,2} + \Theta') \\ &= a_{1,2}^2 - d, \quad d \equiv 2, 3 \pmod 4 \\ &= a_{1,2}^2 + a_{1,2} + \frac{1-d}{4}, \quad d \equiv 1 \pmod 4. \end{aligned}$$

Wenn diese Zahl durch p theilbar ist, so ist einer der beiden Factoren $a_{1,2} + \Theta$, $a_{1,2} + \Theta'$ durch π theilbar. Da aber $\Theta' = -\Theta$ oder $= 1 - \Theta$ ist, also

$$\begin{array}{ll} a) & a_{1,2} + \Theta' = -(-a_{1,2} + \Theta) \\ b) & a_{1,2} + \Theta' = -(-a_{1,2} - 1 + \Theta) \end{array}$$

ist, so kann man $a_{1,2}$ immer so annehmen, dass gerade $a_{1,2} + \Theta$ durch π theilbar wird, und Θ ist also wirklich mit einer rationalen Zahl congruent. Die nothwendige und hinreichende Bedingung dafür, dass p zwei Primfactoren enthält, ist folglich die, dass $a_{1,2}^2 - d$ oder $a_{1,2}^2 + a_{1,2} + \frac{1}{4}(1 - d)$ durch geeignete Annahme über $a_{1,2}$ durch p theilbar wird. Durch Multiplication mit 4 gehen diese beiden Bedingungen über in

$$4\,a_{1,2}^2 - 4\,d \equiv 0, \quad (2\,a_{1,2} + 1)^2 - d \equiv 0 \pmod{4p},$$

und wenn man bedenkt, dass die Grundzahl Δ im Falle a) gleich $4d$, im Falle b) gleich d ist, so erhalten wir, wenn wir

(5) $$x = 2a_{1,2} \quad \text{oder} \quad = 2a_{1,2} + 1$$

setzen, folgendes Resultat:

1. Die nothwendige und hinreichende Bedingung dafür, dass p zwei Primfactoren enthält, ist die, dass die Congruenz

(6) $$x^2 \equiv \Delta \pmod{4p}$$

durch eine ganze rationale Zahl x befriedigt werden kann, oder dass die Grundzahl Δ quadratischer Rest von $4p$ ist.

Bezeichnen wir mit π, π' die beiden conjugirten Formen

(7) $$\pi = pu + (a_{1,2} + \Theta)\,v, \quad \pi' = pu + (a_{1,2} + \Theta')\,v,$$

so ergiebt sich durch Multiplication

(8) $$\pi\pi' = p\left(pu^2 + xuv + \frac{x^2 - \Delta}{4p}\,v^2\right).$$

Hierin ist nun

$$pu^2 + xuv + \frac{x^2 - \Delta}{4p}\,v^2$$

eine Einheit, weil, wenn p in Δ nicht aufgeht, x durch p nicht theilbar ist, und wenn p in Δ aufgeht, zwar x, aber nicht $(x^2 - \Delta : 4p)$ durch p theilbar ist. Denn ist p ungerade, so kann p^2 nicht in Δ aufgehen, und ist $p = 2$ und Δ durch 2 theilbar, so ist $\Delta = 4d$, $d \equiv 2, 3 \pmod 4$. Wäre aber

$$x^2 - \Delta \equiv 0 \pmod{16},$$

so würde folgen

$$d \equiv \left(\frac{x}{2}\right)^2 \pmod 4,$$

während doch $\left(\frac{x}{2}\right)^2$ als Quadrat nicht mit 2 oder 3 congruent sein kann. Demnach ist p in die beiden Primfactoren π und π' zerlegt.

Die beiden Factoren π und π' von p können auch mit einander associirt sein. Dies tritt nur dann ein, wenn π' und folglich auch $\pi - \pi'$ durch π theilbar ist. Nun ist aber nach (7)

$$\pi - \pi' = (\Theta - \Theta')\,v,$$

und folglich muss

$$(\Theta - \Theta')^2 = \Delta$$

durch p theilbar sein, und dies ist auch die hinreichende Bedingung.

2. **Es ist also p nur dann mit dem Quadrat eines Primfunctionals associirt, wenn p in der Grundzahl Δ aufgeht, in Uebereinstimmung mit dem allgemeinen Satze (§. 158).**

§. 166.

Functionale im quadratischen Körper und quadratische Irrationalzahlen.

Wir betrachten nun in unserem quadratischen Körper ein beliebiges ganzes Functional und bilden seine Basisform

$$\varphi = \alpha_1 t_1 + \alpha_2 t_2,$$

indem wir α_1, α_2 nach §. 165 bestimmen:

(1) $$\alpha_1 = a_{1,1}, \quad \alpha_2 = a_{1,2} + a_{2,2}\Theta.$$

Nach §. 146 ist dann

(2) $$N_a(\varphi) = a_{1,1}\, a_{2,2}.$$

Geben wir der Form φ den Ausdruck

(3) $$\varphi = a_{1,1} t_1 + (a_{1,2} + a_{2,2}\Theta)\, t_2,$$

und bilden die Norm, so ergiebt sich

(4) $$N(\varphi) = a_{1,1}^2 t_1^2 + [2\, a_{1,1} a_{1,2} + a_{1,1} a_{2,2} (\Theta + \Theta')]\, t_1 t_2 + t_2^2 N(\alpha_2)$$

und der Theiler dieser Form ist also nach (2) gleich $a_{1,1} a_{2,2}$.

Wenn wir also

(5) $$\begin{aligned} a_{1,1}^2 &= c\; a_{1,1} a_{2,2} \\ 2\, a_{1,1} a_{1,2} + a_{1,1} a_{2,2} (\Theta + \Theta') &= b\; a_{1,1} a_{2,2} \\ N(\alpha_2) &= -\, a\; a_{1,1} a_{2,2} \end{aligned}$$

setzen, so sind a, b, c ganze rationale Zahlen ohne gemeinschaftlichen Theiler, und der Quotient

(6) $$\frac{\alpha_2}{\alpha_1} = \omega$$

ist eine Wurzel der quadratischen Gleichung

(7) $$c\,\omega^2 = a + b\,\omega.$$

Wenn wir in den Ausdrücken (1) die Werthe von $a_{1,1}$ und $a_{1,2}$ aus (5) substituiren, so folgt

(8) $$\begin{aligned} 2\,\alpha_2 &= a_{2,2}\,(b + \Theta - \Theta') \\ \alpha_1 &= c\, a_{2,2}. \end{aligned}$$

Nun ist nach §. 164, (8) die Differenz $\Theta - \Theta'$ gleich der Quadratwurzel aus der Grundzahl von Ω, so dass wir aus (6) und (8) erhalten:

$$(9) \qquad \omega = \frac{b + \sqrt{\Delta}}{2c}, \quad \Delta = b^2 + 4ac,$$

worin das Vorzeichen von $\sqrt{\Delta}$ durch die in §. 164, (6) gemachte Annahme über das Vorzeichen von $\sqrt{d}$ bestimmt ist.

Es ist also ω eine zur Discriminante Δ gehörige quadratische Irrationalzahl, wie wir sie im §. 122 des ersten Bandes betrachtet haben, und die Form φ kann, wenn wir $a_{2,2} = e$ setzen, so ausgedrückt werden:

$$(10) \qquad \varphi = ec\,(t_1 + \omega t_2).$$

Hierin ist c die kleinste positive ganze rationale Zahl, für die das Product $c\,\omega$ eine ganze Zahl wird, und jede andere ganze rationale Zahl k, durch die das Product $k\,\omega$ eine ganze Zahl wird, muss durch c theilbar sein.

Man erkennt dies am einfachsten, wenn man ω nach §. 164, je nachdem b gerade oder ungerade ist, in eine der beiden Formen setzt:

$$(11) \qquad \omega = \frac{1}{c}\left(\frac{b}{2} + \Theta\right), \quad \frac{1}{c}\left(\frac{b-1}{2} + \Theta\right),$$

woraus, da $1, \Theta$ eine Basis von $\mathfrak{o}$ ist, das Gesagte hervorgeht.

Darauf gründet sich nun der Beweis, dass, wenn ω irgend eine zur Discriminante Δ gehörige quadratische Irrationalzahl bedeutet, c die kleinste positive ganze rationale Zahl, die $c\omega$ zu einer ganzen Zahl macht, und e eine beliebige positive ganze rationale Zahl, auch umgekehrt durch

$$(12) \qquad \varphi = ec\,(t_1 + \omega t_2)$$

immer eine Basisform dargestellt ist.

Dazu haben wir nur zu zeigen, dass

$$\alpha_1 = ec, \quad \alpha_2 = ec\,\omega$$

eine Basis des durch (12) definirten Functionals φ ist.

Bilden wir zu diesem Zwecke zunächst die Norm von φ, so erhalten wir nach (7)

$$(13) \qquad N(\varphi) = e^2 c\,(c t_1^2 + b\, t_1 t_2 - a t_2^2),$$

und folglich die absolute Norm

$$(14) \qquad N_a(\varphi) = e^2 c.$$

Ist nun

(15) $$\alpha_1 = a_{1,1}, \quad \alpha_2 = a_{1,2} + a_{2,2}\Theta$$

eine Basis von φ, so ist andererseits (nach §. 146)

(16) $$N_a(\varphi) = a_{1,1}\, a_{2,2},$$

und $a_{1,1}$ ist die kleinste positive ganze rationale Zahl, die durch φ theilbar ist.

Nun können wir andererseits zeigen, dass diese Zahl $= e\,c$ ist, woraus $e\,c = a_{1,1}$, und nach (14) und (16) $e = a_{2,2}$ folgt.

Wenn nämlich eine ganze rationale Zahl m durch φ theilbar sein soll, so muss, wenn ω' zu ω conjugirt ist, da

$$c\,t_1^2 + b\,t_1\,t_2 - a\,t_2^2$$

ein Einheitsfunctional ist,

$$\frac{m\,(c\,t_1^2 + b\,t_1\,t_2 - a\,t_2^2)}{\varphi} = \frac{m}{e}\,(t_1 + \omega' t_2)$$

ein ganzes Functional sein. Folglich müssen

$$\frac{m}{e} \text{ und } \frac{m}{e}\,\omega'$$

ganze Zahlen sein, woraus folgt, dass $m : e$ eine durch c theilbare, also m eine durch $e\,c$ theilbare ganze rationale Zahl ist. Da andererseits $e\,c$ durch φ theilbar ist, so folgt, dass $e\,c$ die kleinste diesen Forderungen genügende Zahl ist. Ausserdem ergiebt sich noch, dass die ganze Zahl $e\,c\,\omega$ durch φ theilbar ist. Denn $e\,c\,\omega$ ist in der Darstellung (12) ein Coëfficient der ganzen Function φ und daher durch φ theilbar (§. 142).

Drücken wir Θ in (15) durch ω aus, so ergiebt sich nach (11)

$$\begin{aligned} \alpha_2 &= a_{1,2} - \frac{e\,b}{2} + e\,c\,\omega, \qquad b \text{ gerade} \\ &= a_{1,2} - \frac{e\,(b-1)}{2} + e\,c\,\omega, \quad b \text{ ungerade,} \end{aligned}$$

und es ist also

$$a_{1,2} \equiv \frac{e\,b}{2} \text{ oder } \equiv \frac{e\,(b-1)}{2}$$

nach dem Modul φ, und folglich, da beide Seiten rational sind, auch nach dem Modul $a_{1,1} = e\,c$. Demnach kann $a_{1,2}$ dem Werthe $\frac{1}{2}\,e\,b$ oder $\frac{1}{2}\,e\,(b-1)$ gleich gesetzt werden, und wir erhalten $\alpha_2 = e\,c\,\omega$, was zu beweisen war.

Um das hierdurch Bewiesene übersichtlich zusammenzufassen, können wir folgende Sätze aussprechen:

1. Ist Ω ein quadratischer Körper mit der Grundzahl Δ, und φ ein ganzes Functional in diesem Körper, so lässt sich eine zur Discriminante Δ gehörige quadratische Irrationalzahl

$$\omega = \frac{b + \sqrt{\Delta}}{2c} \tag{17}$$

und eine positive ganze rationale Zahl e so bestimmen, dass

$$ec(t_1 + \omega t_2) \tag{18}$$

eine Basisform von φ wird. Umgekehrt ist, wenn ω eine beliebige zur Discriminante Δ gehörige quadratische Irrationalzahl ist, die Form (18) immer eine Basisform eines Functionals φ.

§. 167.

Aequivalente Functionale und äquivalente Zahlen.

Wenn nun ω, ω_1 irgend zwei zu der Discriminante Δ gehörige quadratische Irrationalzahlen sind, so erhalten wir zwei Basisformen

$$\begin{aligned} \varphi &= ec(t_1 + \omega t_2) \\ \varphi_1 &= e_1 c_1 (t_1 + \omega_1 t_2). \end{aligned} \tag{1}$$

Wenn nun die beiden Zahlen ω, ω_1 in dem Sinne äquivalent sind, wie wir diesen Begriff im §. 120 des ersten Bandes festgesetzt haben, so ist

$$\omega_1 = \frac{p\omega + q}{r\omega + s}, \tag{2}$$

worin p, q, r, s ganze rationale Zahlen sind, die der Bedingung

$$ps - qr = \pm 1 \tag{3}$$

genügen. Machen wir dann die Substitution (2) in φ_1, so folgt

$$(r\omega + s)\varphi_1 = e_1 c_1 [st_1 + qt_2 + \omega(rt_1 + pt_2)],$$

oder wenn wir

$$u_1 = st_1 + qt_2, \quad u_2 = rt_1 + pt_2 \tag{4}$$

setzen,

$$(r\omega + s)\varphi_1 = e_1 c_1 (u_1 + \omega u_2).$$

Nun ist $ec(u_1 + \omega u_2)$ mit φ associirt, weil (4) eine ganz-

zahlige lineare Substitution mit der Determinante ± 1 ist (§. 147), und folglich sind die beiden Formen

$$(r\omega + s)\, e c \varphi_1, \quad e_1 c_1 \varphi$$

mit einander associirt, und dies hat zur Folge, dass die beiden Formen φ, φ_1 in dem in §. 152 definirten Sinne äquivalent sind. Damit haben wir bewiesen:

2. Wenn die quadratischen Irrationalzahlen ω, ω_1 äquivalent sind, so sind auch die entsprechenden Functionale φ, φ_1 äquivalent.

Es lässt sich aber auch der umgekehrte Satz beweisen:

3. Wenn die Functionale φ, φ_1 äquivalent sind, so sind auch die quadratischen Irrationalzahlen ω und ω_1 äquivalent.

Um diesen Beweis zu führen, bezeichnen wir mit ψ ein Functional der Classe, die zu der Classe von φ reciprok ist, so dass $\varphi\psi$ mit einer Zahl äquivalent ist. Dann können wir setzen:

(5) $$\varphi\psi = \varepsilon\xi,$$

worin ε eine Einheit, ξ eine Zahl in $\mathfrak{o}$ ist. Hierin können wir φ und ψ beide als Basisformen annehmen und demnach

(6) $$\varphi = e c\, (t_1 + t_2\omega), \quad \psi = e' c'\, (t_1 + t_2\eta)$$

setzen, worin e', c', η dieselbe Bedeutung für ψ haben, wie e, c, ω für φ. Wir setzen zur Abkürzung [§. 166, (13)]:

(7) $$N_a(\varphi) = e^2 c = P, \quad N_a(\psi) = e'^2 c' = Q.$$

Wenn wir mit ψ' die zu ψ conjugirte Form bezeichnen, und für den Augenblick die Einheitsform

$$c' t_1^2 + b' t_1 t_2 - a' t_2^2 = \varepsilon_1$$

setzen, so folgt aus (5) durch Multiplication mit ψ':

$$Q\varepsilon_1\varphi = \varepsilon\xi\psi',$$

und folglich

(8) $$\frac{Q\varphi}{\xi} = \frac{\varepsilon}{\varepsilon_1}\psi' = \chi,$$

worin χ und ψ' associirt sind. Setzen wir

(9) $$\frac{Qec}{\xi} = \beta_1, \quad \frac{Qec\omega}{\xi} = \beta_2,$$

so wird

$$\chi = \frac{Q\varphi}{\xi} = \beta_1 t_1 + \beta_2 t_2,$$

und folglich sind β_1, β_2 ganze durch ψ' theilbare Zahlen.

Bilden wir aus (9) die Discriminante $\Delta(\beta_1, \beta_2)$, so erhalten wir

(10) $$\Delta(\beta_1, \beta_2) = \begin{vmatrix} \beta_1, & \beta_2 \\ \beta_1', & \beta_2' \end{vmatrix}^2 = \frac{e^4 c^4 Q^4}{(\xi\xi')^2}(\omega - \omega')^2.$$

Aus (5) und (7) folgt aber

$$\xi\xi' = N(\xi) = PQ = e^2 c Q,$$

und wenn wir noch $\omega - \omega' = \frac{\sqrt{\Delta}}{c}$ setzen, so findet sich

(11) $$\Delta(\beta_1, \beta_2) = Q^2 \Delta.$$

Hieraus folgt aber nach dem Satze §. 147, 2., dass β_1, β_2 eine Basis von ψ' ist.

Andererseits ist nach (6) auch $e'c'$, $e'c'\eta'$ eine Basis von ψ', und folglich lassen sich die ganzen rationalen Zahlen p, q, r, s so bestimmen, dass

(12) $$\beta_1 = \frac{Qec}{\xi} \quad = e'c'(r\eta' + s)$$
$$\beta_2 = \frac{Qec}{\xi}\omega = e'c'(p\eta' + q),$$

und zugleich

(13) $$ps - qr = \pm 1.$$

Aus (12) folgt aber durch Division:

(14) $$\omega = \frac{p\eta' + q}{r\eta' + s},$$

d. h. ω ist mit η' äquivalent.

Ersetzen wir nun φ durch die äquivalente Form φ_1, so besteht eine Gleichung wie (5):

$$\varphi_1 \psi = \varepsilon_1 \xi_1,$$

worin ψ ungeändert geblieben ist. Folglich ist auch ω_1 mit η äquivalent, und mithin sind ω und ω_1 unter einander äquivalent. Das ist aber die in unserem Satze 3. ausgesprochene Behauptung, die also hiermit erwiesen ist.

Hiernach entspricht also jeder Idealclasse des Körpers Ω eine Classe äquivalenter Zahlen ω und umgekehrt, und wir können daher noch den Satz hinzufügen:

4. **Die Anzahl der nicht äquivalenten Irrationalzahlen der Discriminante Δ ist gleich der Anzahl der Formenclassen des Körpers Ω**[1]).

§. 168.

Composition der quadratischen Irrationalzahlen.

Wir haben im §. 166 gesehen, dass zu jedem ganzen Functional φ im Körper Ω eine gewisse quadratische Irrationalzahl ω von der Discriminante Δ gefunden werden kann.

Wir müssen aber jetzt noch untersuchen, inwiefern diese Zahl ω durch den Körper Ω und durch das Functional φ bestimmt ist.

Nach §. 166, (1) ist die Basis von φ

(1) $$\alpha_1 = a_{1,1}, \; \alpha_2 = a_{1,2} + a_{2,2}\Theta$$

dadurch definirt, dass $a_{1,1}$ die kleinste positive ganze rationale Zahl ist, die durch φ theilbar ist, und $a_{2,2}$ ist dann durch

(2) $$N_a(\varphi) = a_{1,1}\, a_{2,2}$$

bestimmt, also sind die beiden Zahlen $a_{1,1}$, $a_{2,2}$ durch φ eindeutig bestimmt. Es fragt sich noch, inwiefern auch $a_{1,2}$ bestimmt ist. Die Zahl $a_{1,2}$ ist aber nach dem Modul φ durch die Congruenz $a_{1,2} + a_{2,2}\Theta \equiv 0$ gegeben, und da $a_{1,2}$ auch eine ganze rationale Zahl sein muss, so ist $a_{1,2}$ bis auf ein Vielfaches von $a_{1,1}$ bestimmt. Dieses Vielfache von $a_{1,1}$ bleibt aber in der That willkürlich, da, wenn α_1, α_2 eine Basis von φ ist, dasselbe für jedes ganze rationale k auch von α_1, $\alpha_2 + k\alpha_1$ gilt.

Da nun $\alpha_2 : \alpha_1 = \omega$ die gesuchte quadratische Irrationalzahl ist, so erhalten wir den Satz:

---

[1]) Nach der am Schlusse des §. 128 des ersten Bandes gemachten Bemerkung über die Gauss'sche Theorie der quadratischen Formen stimmt die Classenzahl der quadratischen Formen nach der Gauss'schen Definition nicht immer überein mit der Anzahl der Idealclassen des Körpers Ω. Um die Uebereinstimmung herzustellen, muss man in manchen Fällen die Idealclassen noch weiter in je zwei Classen theilen. Bei unserer Theorie der Aequivalenz der Zahlen ω, wo die eigentliche nicht von der uneigentlichen Aequivalenz unterschieden wird, ist diese weitere Eintheilung nicht erforderlich. Vergl. Dirichlet-Dedekind, Zahlentheorie. 4. Auflage, S. 578, 584.

5. **Zu jedem ganzen Functional des Körpers Ω gehört eine und nur eine Reihe von quadratischen Irrationalzahlen der Discriminante Δ, und die Zahlen dieser Reihe unterscheiden sich um beliebige ganze rationale Zahlen und sind folglich unter einander äquivalent. Associirte Formen führen auf dieselbe Reihe.**

Wenn φ_1, φ_2 zwei ganze Functionale in Ω bedeuten, und

$$\varphi_1 \varphi_2 = \varphi_3$$

gesetzt wird, so können wir zu jeder dieser drei Formen eine quadratische Irrationalzahl $\omega_1, \omega_2, \omega_3$ bestimmen, und ω_3 ist durch ω_1, ω_2 bis auf eine additive ganze rationale Zahl bestimmt. Man nennt dann ω_3 aus ω_1 und ω_2 componirt oder zusammengesetzt, und setzt in symbolischer Bezeichnung

$$\omega_1 \omega_2 = \omega_3. \tag{3}$$

Ist ψ_1 äquivalent mit φ_1, ψ_2 mit φ_2, so ist nach §. 152 auch $\psi_1 \psi_2 = \psi_3$ mit φ_3 äquivalent.

Wenn nun η_1, η_2, η_3 die durch den Satz 5. zu den Formen ψ_1, ψ_2, ψ_3 gehörigen Irrationalzahlen sind, so bilden nach 3., §. 167 die Zahlen η_1, ω_1; η_2, ω_2; η_3, ω_3 drei Paare äquivalenter Zahlen und wir können daher folgenden Satz aussprechen:

6. **Ersetzt man in einer Composition von quadratischen Irrationalzahlen jedes Element durch eine äquivalente Zahl, so geht auch die componirte Zahl in eine äquivalente über.**

Dadurch sind die Classen der quadratischen Irrationalzahlen einer Discriminante Δ zu einer mit der Gruppe der Idealclassen isomorphen Abel'schen Gruppe verbunden.

Um die aus zwei gegebenen Zahlen componirte Zahl wirklich zu finden, hat man so zu verfahren.

Wir wollen die nach (1) gebildeten Basen der Formen $\varphi_1, \varphi_2, \varphi_3$ so bezeichnen:

$$\begin{array}{lll} \varphi_1) & \alpha_1 = a_{1,1} & \alpha_2 = a_{1,2} + a_{2,2}\Theta \\ \varphi_2) & \beta_1 = b_{1,1} & \beta_2 = b_{1,2} + b_{2,2}\Theta \\ \varphi_3) & \gamma_1 = c_{1,1} & \gamma_2 = c_{1,2} + c_{2,2}\Theta, \end{array}$$

so dass

$$\omega_1 = \frac{\alpha_2}{\alpha_1}, \quad \omega_2 = \frac{\beta_2}{\beta_1}, \quad \omega_3 = \frac{\gamma_2}{\gamma_1}$$

wird. Es ist dann $c_{1,1}$ die kleinste positive ganze rationale Zahl, die durch $\varphi_1 \varphi_2$ theilbar ist, und diese muss jedenfalls ein Theiler von $a_{1,1} b_{1,1}$ sein. Hat man

$$a_{1,1}\, b_{1,1} = k\, c_{1,1},$$

wo k eine positive ganze rationale Zahl ist, so ist, weil $N_a(\varphi_1)\, N_a(\varphi_2) = N_a(\varphi_3)$ sein muss,

$$k\, a_{2,2}\, b_{2,2} = c_{2,2}.$$

Die letzte Zahl $c_{1,2}$ ist dann aus der Congruenz

$$(4) \qquad c_{1,2} + c_{2,2}\, \Theta \equiv 0 \pmod{\varphi_1 \varphi_2}$$

zu bestimmen.

Wenn es nur darauf ankommt, einen Repräsentanten der zusammengesetzten Classe zu finden, so verfährt man am einfachsten so.

Ist φ_1 beliebig angenommen, so kann man (nach §. 152, 6.) φ_2 in seiner Classe so wählen, dass es relativ prim zu $a_{1,1}$ wird. Dann ist auch φ_1 relativ prim zu φ_2 und $b_{1,1}$ relativ prim zu $a_{1,1}$.

Denn haben $a_{1,1}$ und $b_{1,1}$ einen grössten gemeinschaftlichen Theiler d, so ist dieser auch relativ prim zu φ_2, und also ist $b_{1,1} : d$ durch φ_2 theilbar; dies aber widerspricht, wenn $d > 1$ ist, der Definition von $b_{1,1}$. Ebenso folgt auch umgekehrt, dass, wenn $a_{1,1}$ und $b_{1,1}$ relativ prim sind, φ_2 zu $a_{1,1}$ relativ prim ist. Denn wenn keiner der rationalen Primfactoren von $b_{1,1}$ in $a_{1,1}$ aufgeht, so kann auch keiner der in φ_2 aufgehenden Primfactoren in $a_{1,1}$ aufgehen.

In diesem Falle ist nun:

$$(5) \qquad a_{1,1}\, b_{1,1} = c_{1,1}, \quad a_{2,2}\, b_{2,2} = c_{2,2}.$$

Die Congruenz (4) wird dann

$$(6) \qquad c_{1,2} + a_{2,2}\, b_{2,2}\, \Theta \equiv 0 \pmod{\varphi_1 \varphi_2},$$

und da

$$a_{1,2} + a_{2,2}\, \Theta \equiv 0 \pmod{\varphi_1}, \quad b_{1,2} + b_{2,2}\, \Theta \equiv 0 \pmod{\varphi_2}$$

ist, so zerfällt (6) in die beiden Congruenzen:

$$\begin{aligned} c_{1,2} &\equiv b_{2,2}\, a_{1,2} \pmod{\varphi_1} \\ &\equiv a_{2,2}\, b_{1,2} \pmod{\varphi_2}. \end{aligned}$$

Diese Congruenzen sind aber nach §. 138, 13. gleichwerthig mit den gewöhnlichen Zahlencongruenzen

$$(7) \qquad \begin{aligned} c_{1,2} &\equiv b_{2,2}\, a_{1,2} \pmod{a_{1,1}} \\ &\equiv a_{2,2}\, b_{1,2} \pmod{b_{1,1}}, \end{aligned}$$

wodurch $c_{1,2}$ nach dem Modul $c_{1,1}$ bestimmt ist.

Es bleibt nur noch übrig, zu zeigen, wie man φ_2 der hier gestellten Forderung gemäss bestimmen kann. Da zwei Formen, die sich nur durch einen Zahlenfactor von einander unterscheiden, äquivalent sind, so ist φ_2 äquivalent mit

$$c_2\,(t_1 + \omega_2 t_2),$$

[§. 166, (10)] und nehmen wir diese Form für φ_2, so ist $b_{1,1} = c_2$. Die Zahl ω_2 kann man aber unter den mit ihr äquivalenten immer so wählen, dass c_2 zu $a_{1,1}$ relativ prim wird, und dann ist auch $a_{1,1}$ zu φ_2 relativ prim.

Ersetzt man nämlich ω_2 durch

$$\frac{p\,\omega_2 + q}{r\,\omega_2 + s},\quad ps - qr = \pm 1,$$

so geht c_2 nach Bd. I, §. 122, (13) in

$$c_2' = -a_2 r^2 + b_2 rs + c_2 s^2$$

über, und nun kann man über die ganzen rationalen Zahlen r, s so verfügen, dass sie unter einander theilerfremd sind und dass c_2' durch irgend welche gegebene Primzahlen nicht theilbar ist.

Denn ist n eine solche Primzahl, so nehme man, wenn n in a_2 und c_2, also nicht in b_2 aufgeht, r und s durch n untheilbar, wenn n in a_2 nicht aufgeht, s durch n theilbar und r durch n untheilbar, und wenn n in c_2 nicht aufgeht, r durch n theilbar, s durch n untheilbar. (Sind a_2 und c_2 beide nicht durch n theilbar, so hat man zwischen den beiden letzteren Annahmen die Wahl.) Diese Forderungen sind für verschiedene beliebig gegebene Primzahlen n mit einander verträglich, und dann lässt sich p, q aus der Bedingung $ps - qr = \pm 1$ bestimmen.

Diese Gesetze der Composition der quadratischen Irrationalzahlen haben wir hier nur unter der Voraussetzung abgeleitet, dass die Discriminante zugleich die Grundzahl eines quadratischen Körpers ist, d. h. dass Δ Stammdiscriminante ist. Dieselben Gesetze gelten aber auch, mit geringen Modificationen, allgemein [1]).

---

[1]) Gauss, Disquisitiones arithm., Art. 234 ff. Dirichlet-Dedekind, Zahlentheorie. 4. Auflage, §. 187.

Einundzwanzigster Abschnitt.

Kreistheilungskörper.

§. 169.

Zerlegung der Primzahl q in Primfactoren im Kreistheilungskörper $\Omega_{q^\varkappa}$.

Wir machen eine zweite Anwendung der allgemeinen Theorie der algebraischen Zahlen auf die Kreistheilungskörper, und gewinnen dadurch das Mittel, die Theorie der Abel'schen Zahlkörper überhaupt zu einem schönen Abschlusse zu bringen.

Die Betrachtungen, die wir zunächst anzustellen haben, lassen sich mit kleinen Modificationen auf jeden vollen Kreistheilungskörper (§. 18) anwenden. Der Einfachheit halber beschränken wir uns hier aber auf den Fall, dass der Grad der Einheitswurzel eine Primzahlpotenz ist, der für die beabsichtigte Anwendung ausreicht.

Es sei q eine natürliche Primzahl (mit Einschluss von 2) und

$$(1) \qquad m = q^\varkappa$$

eine Potenz von q, deren positiver Exponent $\varkappa$ für $q = 2$ grösser als 1 vorausgesetzt wird.

Es sei ferner r eine primitive m^{te} Einheitswurzel und Ω_m der volle Kreistheilungskörper für den Exponenten m, dessen Grad

$$(2) \qquad \mu = \varphi(m) = q^{\varkappa-1}(q-1)$$

ist (Bd. I, §. 134).

Wir bezeichnen durchweg mit n die μ Zahlen eines vollen Restsystems für den Modul m mit Ausschluss der durch q theilbaren Zahlen, und es sind dann die μ Zahlen r^n die Wurzeln der irreduciblen Gleichung μ^{ten} Grades $f(x) = 0$, worin

$$(3) \qquad f(x) = \frac{x^m - 1}{x^{\frac{m}{q}} - 1} = x^{q^{\varkappa-1}(q-1)} + x^{q^{\varkappa-1}(q-2)} + \cdots + 1$$

zu setzen ist. r ist daher eine ganze Zahl in Ω_m, und ihre Norm ist $= + 1$; folglich ist r eine Einheit.

Ω_m ist ein Normalkörper, der durch die μ Substitutionen

$$s_n = (r, r^n)$$

in sich selber übergeht.

Diese μ Substitutionen s_n bilden eine Abel'sche Gruppe $\mathfrak{N}$, welche die Galois'sche Gruppe des Körpers Ω_m ist. Sie ist isomorph mit der gleichfalls durch $\mathfrak{N}$ zu bezeichnenden Gruppe der nach dem Modul m genommenen Zahlclassen n (§. 16).

Die Function $f(x)$ lässt sich in die μ Factoren $x - r^n$ zerlegen, und wir setzen daher

$$(4) \qquad f(x) = \prod^n (x - r^n).$$

Setzen wir darin $x = 1$, und beachten, dass [nach (3)] $f(1) = q$ ist, so folgt

$$(5) \qquad q = \prod^n (1 - r^n).$$

Die Zahlen

$$(6) \qquad \sigma_n = 1 - r^n, \quad \sigma = 1 - r$$

sind aber ganze Zahlen des Körpers Ω_m, und die Formel (5) zeigt zunächst, dass q im Körper Ω_m in μ Factoren σ_n zerlegbar ist.

Wir beweisen zunächst, dass die μ Zahlen σ_n mit einander associirt sind. Bedeuten n, n' zwei durch q nicht theilbare Zahlen, so können wir eine natürliche Zahl a so bestimmen, dass

$$n' \equiv a\,n \pmod{m}$$

wird. Dann ist aber

$$\frac{\sigma_{n'}}{\sigma_n} = \frac{1 - r^{an}}{1 - r^n} = 1 + r^n + r^{2n} + \cdots + r^{(a-1)n}$$

eine ganze Zahl, also $\sigma_{n'}$ durch σ_n theilbar. Da hierin n mit n' vertauscht werden kann, so ist auch σ_n durch $\sigma_{n'}$ theilbar, also sind beide Zahlen associirt (§. 138). Wenn daher ε eine Einheit bedeutet, so ist nach (5):

$$(7) \qquad q = \varepsilon\,\sigma^\mu, \quad N(\sigma) = q.$$

Es ist also die natürliche Primzahl q associirt mit der μ^{ten} Potenz einer ganzen Zahl σ im Körper Ω_m. Diese Zahl σ ist aber auch im Körper Ω_m noch Primzahl, und zwar vom ersten Grade. Denn hat σ irgend einen Theiler σ', so muss die Norm von σ' ein Theiler der Norm von σ sein, also, wenn σ' keine

Einheit ist, so ist $N(\sigma') = q$. Folglich ist die Norm von $\sigma : \sigma'$ gleich 1, d. h. $\sigma : \sigma'$ ist eine Einheit und σ mit σ' associirt. Wir haben also den ersten Satz:

I. Die natürliche Primzahl q ist in dem vollen Kreistheilungskörper Ω_m mit der μ^{ten} Potenz eines Primfactors ersten Grades associirt.

Wenn wir mit m_1 einen Theiler von m bezeichnen, kleiner als m und grösser als 1, und

(8) $$m = m_1 m_2$$

setzen, so dass m_1 und m_2 selbst Potenzen von q sind, so ergiebt sich die Zerlegung:

$$x^{m_1} - 1 = (x - 1)(x r^{m_2} - 1)(x r^{2 m_2} - 1) \ldots (x r^{(m_1 - 1) m_2} - 1),$$

und wenn wir darin $x = r$ setzen, nach (6):

(9) $$r^{m_1} - 1 = (-1)^{m_1} \prod_{0, m_1 - 1}^{s} \sigma_{1 + s m_2},$$

und daraus, da μ immer gerade ist,

(10) $$N(r^{m_1} - 1) = q^{m_1}.$$

Hiernach lässt sich leicht die Discriminante Δ der Gleichung (3) bilden, die nach Bd. I, §. 47 den Ausdruck hat:

$$\Delta = (-1)^{\frac{\mu(\mu - 1)}{2}} N f'(r).$$

Es ist nämlich nach (3):

$$f'(r) = \frac{m\, r^{m-1}}{r^{\frac{m}{q}} - 1},$$

also, da die Norm von r gleich 1 ist:

$$N f'(r) = \frac{m^{\mu}}{q^{\frac{m}{q}}},$$

und folglich (da μ immer gerade ist):

(11) $$\Delta = (-1)^{\frac{\mu}{2}} q^{q^{\varkappa - 1} [\varkappa (q - 1) - 1]}.$$

Die Discriminante Δ ist also, vom Vorzeichen abgesehen, eine Potenz von q.

§. 170.

Minimalbasis des Körpers Ω_m.

Die Sätze, die im vorigen Paragraphen bewiesen sind, führen uns zu dem folgenden Theorem:

II. Die Zahlen

(1) $$1, r, r^2, \ldots, r^{\mu-1}$$

bilden eine Basis des Systemes $\mathfrak{o}$ der ganzen Zahlen in Ω_m.

Um dies zu zeigen, genügt nach §. 145 der Nachweis, dass die ganze Zahl in Ω_m

(2) $$\omega = x_0 + x_1 r + x_2 r^2 + \cdots + x_{\mu-1} r^{\mu-1},$$

worin $x_0, x_1, \ldots, x_{\mu-1}$ ganze rationale Zahlen sind, nur dann durch eine rationale Primzahl p theilbar sein kann, wenn die Zahlen $x_0, x_1, \ldots, x_{\mu-1}$ alle durch p theilbar sind.

Nehmen wir also an, es sei ω durch p theilbar; dann sind auch alle Zahlen ω_n, die aus ω durch eine der μ Substitutionen (r, r^n) entstehen, durch p theilbar, und wir erhalten also aus (2) ein System von μ Gleichungen, die in Bezug auf die x_i linear sind:

(3) $$\omega_n = x_0 + x_1 r^n + x_2 r^{2n} + \cdots + x_{\mu-1} r^{(\mu-1)n}.$$

Die Determinante dieses Systemes, d. h. die aus den μ Reihen

$$1, r^n, r^{2n}, \ldots, r^{(\mu-1)n}$$

gebildete Determinante ist aber nach Bd. I, §. 46 gleich der Quadratwurzel $\sqrt{\Delta}$, und wenn wir also das System der Gleichungen (3) auflösen, so folgt, dass die sämmtlichen rationalen Zahlen $\Delta\, x_i$ durch p theilbar sein müssen.

Ist nun p nicht $= q$, so ist Δ nicht durch p theilbar, und sämmtliche x_i müssen durch p theilbar sein.

Ist aber $p = q$, so setzen wir

$$f(t) = x_0 + x_1 t + x_2 t^2 + \cdots + x_{\mu-1} t^{\mu-1},$$

so dass $\omega_n = f(r^n)$ wird, und setzen darin $r = 1 - \sigma$ [§. 169, (6)]. Dann ist nach der Taylor'schen Entwickelung:

(4) $$\omega = f(1-\sigma) = f(1) - \sigma f'(1) + \frac{\sigma^2}{1.2} f''(1) - \cdots$$
$$- \frac{\sigma^{\mu-1}}{\Pi(\mu-1)} \overset{(\mu-1)}{f}(1).$$

und hierin sind die Coëfficienten

$$f(1), f'(1), \tfrac{1}{2}f''(1), \ldots, \frac{1}{\Pi(\mu-1)} \overset{(\mu-1)}{f(1)}$$

ganze rationale Zahlen, nämlich

$$\begin{aligned}
\frac{1}{\Pi(\mu-1)} \overset{(\mu-1)}{f(1)} &= x_{\mu-1} \\
\frac{1}{\Pi(\mu-2)} \overset{(\mu-2)}{f(1)} &= x_{\mu-2} + (\mu-1)\, x_{\mu-1} \\
(5) \quad \frac{1}{\Pi(\mu-3)} \overset{(\mu-3)}{f(1)} &= x_{\mu-3} + (\mu-2)\, x_{\mu-2} + \frac{(\mu-1)(\mu-2)}{1.2}\, x_{\mu-1} \\
\ldots & \ldots \\
f(1) &= x_0 + x_1 + \cdots + x_{\mu-1}.
\end{aligned}$$

Da nun ω durch q und folglich durch σ^μ theilbar ist, so muss $f(1)$ nach (4) durch q theilbar sein. Da aber $\mu > 1$ und folglich $q : \sigma$ noch durch σ theilbar ist, so folgt, dass auch

$$f'(1) - \frac{\sigma}{1.2} f''(1) \ldots$$

durch σ, folglich $f'(1)$ durch q theilbar ist, und wenn man so weiter schliesst, ergiebt sich, dass die sämmtlichen rationalen Zahlen (5) durch q theilbar sind, und folglich sind auch die $x_{\mu-1}, x_{\mu-2}, \ldots, x_0$ durch q theilbar. Damit ist der Satz II. vollständig bewiesen.

Anstatt der Reihe (1) kann man auch eine beliebige Reihe von μ auf einander folgenden Potenzen von r als Basis von $\mathfrak{o}$ nehmen:

(6) $$r^a,\ r^{a+1},\ r^{a+2}, \ldots, r^{a+\mu-1},$$

die sich ergiebt, wenn man alle Glieder der Reihe (1) mit r^a multiplicirt.

Die Richtigkeit dieser Bemerkung ergiebt sich daraus, dass die $r^{\pm a}$ ganze Zahlen sind, und dass also ω und $r^a \omega$ stets gleichzeitig ganze oder gebrochene Zahlen sind.

Beispielsweise bilden die Zahlen

(7) $$r^{-\frac{1}{2}\mu+1},\ r^{-\frac{1}{2}\mu+2}, \ldots, r^{-1},\ 1,\ r,\ r^2, \ldots, r^{\frac{1}{2}\mu}$$

eine Basis von $\mathfrak{o}$.

Damit ist auch die Grundzahl Δ des Körpers Ω_m bestimmt. Sie ist nach der allgemeinen Definition (§. 145) gleich der Discriminante

$$\Delta(1, r, r^2, \ldots, r^{\mu-1}),$$

d. h. gleich der in §. 169 bestimmten Discriminante der Kreistheilungsgleichung.

§. 171.

Die Primideale im Körper Ω_m.

Wir haben im §. 164 gesehen, dass die natürliche Primzahl q die μ^{te} Potenz einer Primzahl σ im Körper Ω_m ist.

Um alle Primideale, die im Körper Ω_m existiren, zu ermitteln, sind also noch sämmtliche von q verschiedene natürliche Primzahlen p in Primfactoren zu zerlegen, und es sind darunter die nicht associirten auszusuchen.

Die Grundlage für diese Untersuchung bilden die Sätze des §. 162, wenn der dort mit R bezeichnete Körper durch den Körper der rationalen Zahlen ersetzt wird.

Jede Zahl ω des Körpers Ω_m geht durch eine der μ Substitutionen

$$s_n = (r, r^n)$$

in eine bestimmte andere Zahl ω_n über, die gleichfalls in Ω_m enthalten ist. Ist

(1) $$\omega = \omega_1 = a_0 + a_1 r + a_2 r^2 + \cdots + a_{\mu-1} r^{\mu-1},$$

so ist

(2) $$\omega_n = a_0 + a_1 r^n + a_2 r^{2n} + \cdots + a_{\mu-1} r^{(\mu-1)n}.$$

Wenn eine dieser Zahlen ω_n eine ganze Zahl ist, wie wir jetzt annehmen wollen, so sind es auch alle anderen, und dies tritt immer dann und nur dann ein, wenn die rationalen Zahlen $a_0, a_1, \ldots, a_{\mu-1}$ ganz sind.

Sind h, k irgend zwei Exponenten, so ist

$$r^h - r^k = r^k (r^{h-k} - 1),$$

und dies ist nach §. 169, (9) mit einer Potenz von σ associirt, also, wenn $\mathfrak{p}$ ein in p aufgehendes Primideal bedeutet, durch $\mathfrak{p}$ nicht theilbar, ausser wenn $h \equiv k \pmod{m}$ ist. Daraus ergiebt sich, dass zwei Zahlen ω_h, ω_k, nur dann nach dem Modul $\mathfrak{p}$ congruent sein können, wenn $h \equiv k \pmod{m}$ ist, und dass also die Gruppe X des §. 162, die der Bedingung

$$\omega \,|\, \chi \equiv \omega \pmod{\mathfrak{p}}$$

genügt, nur die identische Substitution enthält. Daraus folgt aber, dass $g = 1$, d. h. dass p nicht durch das Quadrat eines Primideales theilbar ist.

Bilden wir aus (2) die p^{te} Potenz von ω, und beachten den **Fermat'**schen Lehrsatz für rationale Zahlen $[a_0^p \equiv a_0 \pmod{p}]$, so ergiebt sich

$$\omega^p \equiv a_0 + a_1 r^p + a_2 r^{2p} + \cdots + a_{\mu-1} r^{(\mu-1)p} \pmod{p},$$

oder nach (2)

(3) $$\omega^p \equiv \omega_p \pmod{p}.$$

Dadurch ist die Gruppe Ψ bestimmt, zu der das Ideal $\mathfrak{p}$ gehört. Es ist nämlich nach (3) auch

$$\omega^p \equiv \omega_p \pmod{\mathfrak{p}},$$

daher ist $\psi_0 = (r, r^p)$ und die Gruppe Ψ besteht nach §. 162, (13) aus den Potenzen dieser Substitution, soweit sie von einander verschieden sind.

Ist daher f der kleinste positive Exponent, für den

(4) $$p^f \equiv 1 \pmod{m}$$

ist, d. h. gehört p zu dem Exponenten f für den Modul m, so ist

(5) $$\Psi = (r, r), (r, r^p), (r, r^{p^2}), \ldots (r, r^{p^{f-1}})$$

und ist vom f^{ten} Grade. Demnach ist auch $\mathfrak{p}$ ein Primideal f^{ten} Grades und

(6) $$N(\mathfrak{p}) = p^f.$$

Die Anzahl e der von einander verschiedenen conjugirten Primfactoren von f ist $\mu : f$, und wir haben also den Satz:

III. Ist p eine von q verschiedene Primzahl, die für den Modul m zum Exponenten f gehört, ist ferner $\mu = \varphi(m) = ef$, so zerfällt p in Ω_m in e von einander verschiedene conjugirte Primfactoren f^{ten} Grades.

§. 172.

Die conjugirten Primideale.

Wir müssen noch etwas genauer auf die Bildung der conjugirten Primfactoren $\mathfrak{p}_n$ einer von q verschiedenen Primzahl p eingehen, die nach dem zuletzt bewiesenen Satze in Ω_m in e von einander verschiedene Primfactoren zerfällt, wenn

(1) $$\varphi(m) = ef$$

ist, und f der kleinste positive Exponent, für den

(2) $$p^f \equiv 1 \pmod{m}.$$

Die Gruppe Ψ ist isomorph mit einer in $\mathfrak{R}$ (§. 169) enthaltenen Gruppe nach dem Modul m genommener ganzer rationaler Zahlen, die wir mit $\mathfrak{A}$ bezeichnen, die aus allen, einer Congruenz

(3) $$a \equiv p^h \pmod{m}$$

genügenden Zahlen a besteht, und die wir daher symbolisch durch

(4) $$\mathfrak{A} \equiv p^h \pmod{m}$$

darstellen können, wenn h einen beliebigen ganzzahligen Exponenten bedeutet (vergl. §. 18).

Wir können also, wenn wir die Zahlen $\xi_1, \xi_2, \ldots, \xi_e$ aus $\mathfrak{R}$ passend auswählen:

(5) $$\mathfrak{R} = \mathfrak{A}\xi_1 + \mathfrak{A}\xi_2 + \mathfrak{A}\xi_3 + \cdots + \mathfrak{A}\xi$$

setzen, und jeder dieser Nebengruppen entspricht eines der conjugirten Functionale $\mathfrak{p}_{\xi_1}, \mathfrak{p}_{\xi_2}, \ldots, \mathfrak{p}_{\xi_e}$, die alle von einander verschieden sind und deren Product mit p associirt ist.

Wir setzen also

(6) $$p = \mathfrak{p}_{\xi_1}\mathfrak{p}_{\xi_2} \ldots \mathfrak{p}_{\xi_e}.$$

Um aber das Zahlensystem

(7) $$\xi_1, \xi_2, \ldots, \xi_e,$$

auf das es hauptsächlich ankommt, genauer zu charakterisiren, bemerken wir, dass wir dazu jedes System von e Zahlen der Gruppe $\mathfrak{R}$ nehmen können, wenn nur keine zwei unter ihnen, ξ, ξ', eine Congruenz

$$\xi'\xi^{-1} \equiv p^h \pmod{m}$$

erfüllen.

Um ein solches Zahlensystem zu finden, ist es gut, den Fall eines ungeraden m von dem anderen zu trennen, in dem m eine Potenz von 2 ist.

1. Ist zunächst $m = q^\varkappa$ ungerade, so nehmen wir eine primitive Wurzel g von m (§. 14) und setzen

(8) $$p \equiv g^\gamma \pmod{m}.$$

Denn f ist [nach (1), (2)] die kleinste positive Zahl, die der Bedingung

$$\gamma f \equiv 0 \pmod{\mu}$$

genügt, und folglich ist e der grösste gemeinschaftliche Theiler von μ und γ, und irgend eine Zahl $n \equiv g^\lambda$ ist nur dann mit

einer Potenz von p congruent, wenn λ durch e theilbar ist. Denn nur dann kann die Congruenz

$$\lambda \equiv \gamma x \pmod{\mu}$$

befriedigt werden. Setzen wir

$$\gamma = e\,\nu,$$

so ist ν relativ prim zu f. Daraus folgt, dass die Reihe der Zahlen

$$(9) \qquad 1, g, g^2, \ldots, g^{e-1}$$

für die ξ genommen werden kann. Denn sind h, h' zwei verschiedene Zahlen der Reihe $0, 1, 2, \ldots, e-1$, so ist $h'-h$ niemals durch e theilbar, und folglich

$$\xi' \xi^{-1} = g^{h'-h}$$

niemals mit einer Potenz von p congruent.

Wir wollen ferner noch die beiden Fälle unterscheiden, dass $p-1$ durch q theilbar ist oder nicht.

a) Ist $p \equiv 1 \pmod{q}$, so ist $\gamma \equiv 0 \pmod{q-1}$, und folglich e theilbar durch $q-1$. Wir können daher

$$e = \varphi(q^{\varkappa_1}) = q^{\varkappa_1 - 1}(q-1)$$

setzen, worin $0 < \varkappa_1 \lesseqgtr \varkappa$ ist.

Wenn $\varkappa_1 = \varkappa$, also $e = \varphi(m)$, $f = 1$, und daher $p-1$ durch m theilbar ist, so durchläuft ξ die ganze Gruppe $\mathfrak{R}$, und alle Primfunctionale $\mathfrak{p}_n$ sind von einander verschieden.

Ist $\varkappa_1 < \varkappa$, so ist ν durch q nicht theilbar, weil sonst e nicht der grösste gemeinschaftliche Theiler von μ und γ wäre, und

$$p - 1 \equiv g^{\nu\varphi(q^{\varkappa_1})} - 1 \pmod{m}$$

ist durch $q^{\varkappa_1}$ theilbar, aber durch keine höhere Potenz von q. Setzen wir also $q^{\varkappa_1} = m_1$ und

$$(10) \qquad m = m_1 m_2,$$

so ist m_1 der grösste gemeinschaftliche Theiler von $p-1$ und m. Die Primzahl p zerfällt im Körper Ω_m in $\varphi(m_1)$ verschiedene Primfactoren. In ebenso viele Primfactoren zerfällt aber p auch im Körper Ω_{m_1}, der ein Theiler des Körpers Ω_m ist und aus allen rationalen Functionen der m_1^{ten} Einheitswurzel $r_1 = r^{m_2}$ besteht. Daraus folgt, dass die Primfactoren von p in Ω_{m_1} auch im Körper Ω_m nicht weiter zerlegbar sind, und dass wir daher die Primfactoren $\mathfrak{p}$ in Ω_m als Functionale des Körpers Ω_{m_1} darstellen können.

Es durchläuft ξ ein volles System durch q nicht theilbarer Reste nach dem Modul m_1, und die $\mathfrak{p}_\xi$ sind Ideale in Ω_{m_1}.

b) Ist umgekehrt γ durch $q - 1$ theilbar, so folgt aus (8), dass $p - 1$ durch q theilbar ist. Nehmen wir also $p - 1$ nicht durch q theilbar an, so ist auch e nicht durch $q - 1$ theilbar, und ξ durchläuft die Reihe der Zahlen (9).

Bilden wir die Summe dieser Zahlen ξ, so folgt:

$$(g - 1) \sum \xi \equiv g^e - 1 \pmod{m},$$

und diese Zahl ist durch q theilbar oder nicht theilbar, je nachdem e durch $q - 1$ theilbar oder nicht theilbar ist. Da ausserdem $g - 1$ nicht durch q theilbar ist, so ist $\sum \xi$ durch q theilbar oder nicht theilbar, je nachdem $p - 1$ durch q theilbar oder nicht theilbar ist.

2. Wir wenden uns zu dem Falle, dass $m = 2^\varkappa$ eine Potenz von 2 ist, und hier haben wir wieder zu unterscheiden, ob $p - 1$ durch 4 oder nur durch 2 theilbar ist.

a) Ist $p - 1$ durch 4 theilbar, so ist (§. 15):

$$p \equiv 5^\beta \pmod{m},$$

und f ist die kleinste positive Zahl, die der Bedingung

$$\beta f \equiv 0 \left[\operatorname{mod} \tfrac{1}{2}\varphi(m)\right]$$

genügt. Ist $f = 1$, also β durch $\frac{1}{2}\varphi(m) = 2^{\varkappa - 2}$ theilbar, so ist $e = \varphi(m)$, und ξ durchläuft die ganze Gruppe $\mathfrak{R}$, d. h. alle ungeraden Zahlen zwischen 0 und m. Dies ist der Fall, wo $p - 1$ durch m theilbar ist.

Ist $2^{\varkappa_1 - 2}$ die höchste Potenz von 2, die in β aufgeht, und $2 \leqq \varkappa_1 < \varkappa$, so ist, wenn wir $m_1 = 2^{\varkappa_1}$ und $m = m_1 m_2$ setzen,

$$f = 2^{\varkappa - \varkappa_1}, \quad e = 2^{\varkappa_1 - 1} = \varphi(m_1),$$

und es ist, wenn s eine ungerade Zahl ist,

$$p - 1 \equiv 5^{s\, {}^1\!/_2 \varphi(m_1)} - 1 \ldots \pmod{m}.$$

Nach §. 15 ist $5^{{}^1\!/_2 \varphi(m_1)} - 1$ durch m_1, aber durch keine höhere Potenz von 2 theilbar. Da man ausserdem nach denselben Sätzen

$$5^{s\, {}^1\!/_2 \varphi(m_1)} \equiv 5^{{}^1\!/_2 \varphi(m_1)} \pmod{2 m_1}$$

hat, so folgt, dass m_1 der grösste gemeinschaftliche Theiler von $p - 1$ und m ist.

Wenn wir also, wie oben, den Körper Ω_{m_1} zuziehen, so ergiebt sich, dass, wenn $m_1 \geqq 4$ der grösste gemeinschaftliche Theiler von $p - 1$ und m ist, ξ ein volles System ungerader Reste von m_1 durchläuft, und dass $\mathfrak{p}_\xi$ zugleich die Primfactoren von p im Körper Ω_{m_1} sind.

b) Ist $p - 1$ nicht durch 4 theilbar, also

(11) $$p \equiv -5^{\beta} \pmod{m},$$

so ist f die kleinste positive Zahl, die den Congruenzen

$$f \equiv 0 \pmod{2}, \quad 2\beta f \equiv 0 \; [\mathrm{mod}\; \varphi(m)]$$

genügt, und folglich ist e der grösste gemeinschaftliche Theiler von $\varphi(m)$ und 2β, oder, wenn 2β durch $\varphi(m)$ theilbar ist, gleich $\frac{1}{2}\varphi(m)$. (Eine Ausnahme bildet hier der Fall $m = 4$, in dem $e = 1$ ist. Diesen Fall, der ja schon in früheren Abschnitten vollständig erledigt ist, lassen wir daher jetzt bei Seite.)

Es ergiebt sich dann aus (11), dass eine Zahl von der Form 5^{λ} nur dann einer Potenz von p congruent sein kann, wenn λ ein Vielfaches von 2β, also ein Vielfaches von e ist.

Hier kann nun in jeder der Nebengruppen $\mathfrak{A}\xi$ eine Zahl gefunden werden, die $\equiv 1 \pmod{4}$ ist, da $p \equiv -1 \pmod{4}$ eine Zahl in $\mathfrak{A}$ ist, und wir erhalten demnach ein vollständiges System der ξ in der Form:

$$1, 5, 5^2, \ldots, 5^{e-1},$$

und darin ist e höchstens $= \frac{1}{2}\varphi(m) = 2^{\varkappa-2}$.

Wir fassen das Bewiesene im folgenden Theorem zusammen:

III. Zerlegt man die von q verschiedene Primzahl p im Körper Ω_m in ihre Primfactoren:

$$p = \mathfrak{p}_{\xi_1}\mathfrak{p}_{\xi_2}\cdots\mathfrak{p}_{\xi_e},$$

so kann man, wenn $p - 1$ durch q, oder im Falle eines geraden m durch 4 theilbar ist, die ξ ein volles System durch q nicht theilbarer Reste nach dem Modul m_1 durchlaufen lassen, und die $\mathfrak{p}_\xi$ als Primfunctionale im Körper Ω_{m_1} annehmen, wenn m_1 der grösste gemeinschaftliche Theiler von $p - 1$ und m ist.

Ist aber $p - 1$ nicht durch q oder für ein gerades m nicht durch 4 theilbar, und bedeutet g im ersten Falle eine Primitivwurzel von m, im zweiten Falle die Zahl 5, so durchläuft ξ die Reihe der Zahlen

$$1, g, g^2, \ldots, g^{e-1},$$

und e ist bei einem ungeraden m nicht durch $q - 1$ theilbar, und bei geradem m mindestens $= 2$ und höchstens $= \frac{1}{2}\varphi(m)$. Ausgeschlossen ist hierbei der Fall $m = 4$.

§. 173.

Darstellung der Primfactoren von p.

Zur Darstellung der Primfunctionale des Körpers Ω_m können wir ein Verfahren anwenden, was wir im §. 157 kennen gelernt haben, welches sich hier in Folge des Umstandes, dass

$$1, r, r^2, \ldots, r^{\mu-1}$$

eine Basis von $\mathfrak{o}$ ist, wesentlich vereinfacht.

Die natürliche Primzahl q ist, wie wir schon gesehen haben, die m^{te} Potenz einer im Körper Ω_m existirenden Primzahl σ; mit dieser brauchen wir uns nicht weiter zu beschäftigen, und betrachten daher hier nur die von q verschiedenen Primzahlen p. Es sei $\mathfrak{p}$ ein Primfactor von p, und $\mathfrak{A}$ habe dieselbe Bedeutung wie oben. Wenn p zum Exponenten f gehört und

$$ef = \varphi(m) = \mu$$

ist, so besteht die Gruppe $\mathfrak{A}$ aus den Zahlen

$$1, p, p^2, \ldots, p^{f-1}.$$

Wenn nun

$$f(t) = N(t-r) = \prod^{n} (t - r^n)$$

das Polynom von t vom Grade μ bedeutet, dessen Wurzeln die μ Grössen r^n sind, so können wir dies so in Factoren zerlegen, dass jeder Factor einer der Nebengruppen von $\mathfrak{A}$ entspricht. Setzen wir nämlich

$$(1) \qquad F_1(t) = \prod_{0,f-1}^{h} (t - r^{p^h}),$$

und allgemein für jedes durch q nicht theilbare n

$$(2) \qquad F_n(t) = \prod_{0,f-1}^{h} (t - r^{np^h}),$$

so ist $F_n(t)$ mit $F_{n'}(t)$ identisch, wenn n und n' in dieselbe Nebengruppe $\mathfrak{A}\xi_i$ gehören. Wenn wir also mit $\xi_1, \xi_2, \ldots, \xi_e$ das im §. 172, (5) angewandte Zahlensystem verstehen, so ist

$$(3) \qquad f(t) = F_{\xi_1}(t)\, F_{\xi_2}(t) \ldots F_{\xi_e}(t).$$

Nun ist aber nach dem binomischen Lehrsatze:

$$(t - r^{p^h})^p \equiv (t^p - r^{p^{h+1}}) \pmod{p},$$

und wenn wir dies auf jeden Factor von $F_n(t)$ anwenden, und beachten, dass p^{h+1} nach dem Modul m dieselbe Zahlenreihe durchläuft, wie p^h, so folgt:

$$[F_n(t)]^p \equiv F_n(t^p) \pmod{p},$$

und diese Congruenz gilt dann natürlich auch für den Modul $\mathfrak{p}$.

Dies ist aber das Kennzeichen dafür, dass $F_n(t)$ mit einem Polynom $P_n(t)$ mit ganzen rationalen Zahlencoëfficienten nach dem Modul $\mathfrak{p}$ congruent ist (§. 150, 4.), also

(4) $$F_n(t) \equiv P_n(t) \pmod{\mathfrak{p}}.$$

Setzen wir dies in (3) ein, so ergiebt sich zunächst eine Congruenz nach dem Modul $\mathfrak{p}$, die aber, da es eine Congruenz zwischen rationalen Functionen ist, auch für den Modul p bestehen muss, also

(5) $$f(t) \equiv P_{\xi_1}(t)\, P_{\xi_2}(t) \ldots P_{\xi_e}(t) \pmod{p}.$$

Nach der Definition (1), (4) ist

(6) $$P_1(r) \equiv 0 \pmod{\mathfrak{p}},$$

und die sämmtlichen Wurzeln dieser Congruenz sind

(7) $$r,\ r^p, \ldots,\ r^{p^{f-1}}.$$

Ebenso hat die Congruenz

$$P_n(t) \equiv 0 \pmod{\mathfrak{p}}$$

die Wurzeln

$$r^n,\ r^{np}, \ldots,\ r^{np^{f-1}},$$

und diese Wurzeln sind, wenn man n das System der Zahlen $\xi_1, \xi_2, \ldots, \xi_e$ durchlaufen lässt, alle incongruent nach dem Modul $\mathfrak{p}$.

Macht man in der Congruenz

$$F_1(t) \equiv P_1(t) \pmod{\mathfrak{p}}$$

die Substitution (r, r^n), so geht $F_1(t)$ in $F_n(t)$, $\mathfrak{p}$ in das conjugirte Ideal $\mathfrak{p}_n$ über, und $P_1(t)$ bleibt als rationale Form ungeändert. Wir haben also

(8) $$F_n(t) \equiv P_1(t) \pmod{\mathfrak{p}_n},$$

und wenn wir hierin $t = r$ setzen, so folgt:

(9) $$F_n(r) \equiv P_1(r) \pmod{\mathfrak{p}_n},$$

$F_n(r)$ ist aber, wenn n nicht in $\mathfrak{A}$ enthalten ist, relativ prim zu p, also nicht durch $\mathfrak{p}_n$ theilbar.

Es ist also $P_1(r)$ nach (9) durch $\mathfrak{p}_1$, aber durch keinen der

mit $\mathfrak{p}_1$ conjugirten Primfactoren theilbar, und es folgt, da p nicht durch $\mathfrak{p}^2$ theilbar ist:

1. Der Primfactor $\mathfrak{p}_1$ ist der grösste gemeinschaftliche Theiler von p und $P_1(r)$; in gleicher Weise ergiebt sich, dass $\mathfrak{p}_n$ der grösste gemeinschaftliche Theiler von p und $P_1(r^n)$ ist, oder auch der grösste gemeinschaftliche Theiler von p und $P_{n'}(r)$, wenn $n n' \equiv 1 \pmod{m}$ ist.

Das letztere ergiebt sich aus der aus (4) durch die Substitution $(r, r^{n'})$ folgenden Congruenz

$$F_1(t) \equiv P_n(t) \pmod{\mathfrak{p}_{n'}}.$$

Man erhält also die sämmtlichen Primfactoren von p, wenn man die grössten gemeinschaftlichen Theiler von p mit jeder der rationalen Functionen

(10) $$P_{\xi_1}(r),\ P_{\xi_2}(r), \ldots,\ P_{\xi_e}(r)$$

aufsucht, und zwar ist $\mathfrak{p}_{\xi_i}$ der grösste gemeinschaftliche Theiler von p und $P_{\xi_i^{-1}}$.

Wir wollen den Fall noch etwas näher betrachten, wo $f = 1$ ist, also

(11) $$p \equiv 1 \pmod{m}.$$

In diesem Falle ist $e = \varphi(m)$; die Gruppe $\mathfrak{A}$ reducirt sich auf die Einheit, und die sämmtlichen μ conjugirten Factoren $\mathfrak{p}$ von p sind von einander verschieden. Die Formen

$$P_{\xi_1}(t),\ P_{\xi_2}(t), \ldots,\ P_{\xi_e}(t)$$

werden alle linear, d. h. r ist einer rationalen Zahl nach jedem der Moduln $\mathfrak{p}_i$ congruent.

Dies ergiebt sich auch daraus, dass hier die Anzahl der nach dem Modul $\mathfrak{p}$ incongruenten Zahlen gleich $N(\mathfrak{p}) = p$ ist, und dass also $0, 1, 2, \ldots, p - 1$ ein volles Restsystem ist.

Ist hiernach etwa $r \equiv c \pmod{\mathfrak{p}}$, so muss, da $r^m = 1$ ist, $c^m \equiv 1 \pmod{\mathfrak{p}}$ also auch $\pmod{p}$ sein, und wenn also g eine primitive Wurzel der Primzahl p ist, so muss

(12) $$c \equiv g^{-n\frac{p-1}{m}} \pmod{p}$$

sein, worin n relativ prim zu m ist. Lassen wir $\mathfrak{p}$ das System der conjugirten Ideale durchlaufen, so muss n in (12) die Gruppe $\mathfrak{R}$ durchlaufen, und es ist also nur Sache der Bezeichnung, wenn wir festsetzen:

(13) $$r \equiv g^{-\frac{p-1}{m}} \pmod{\mathfrak{p}}.$$

Machen wir darin die Substitution (r, r^n), so wird

(14) $$r^n \equiv g^{-\frac{p-1}{m}} \pmod{\mathfrak{p}_n},$$

oder wenn wir n' durch die Congruenz

(15) $$n n' \equiv 1 \pmod{m}$$

definiren:

(16) $$r \equiv g^{-n'\frac{p-1}{m}} \pmod{\mathfrak{p}_n}.$$

Es ist also in diesem Falle, übereinstimmend mit der allgemeinen Regel, $\mathfrak{p}_n$ der grösste gemeinschaftliche Theiler von

$$p \text{ und } \left(r - g^{-n'\frac{p-1}{m}}\right).$$

Durch diese Bestimmung sind die einzelnen Primformen $\mathfrak{p}_n$ genau charakterisirt. Wir erhalten also den Satz:

2. Eine Primzahl p, die nach dem Modul m mit 1 congruent ist, zerfällt im Körper Ω_m in $\varphi(m)$ von einander verschiedene Primfactoren $\mathfrak{p}_n$ vom ersten Grade, die man als grösste gemeinschaftliche Theiler von p mit den verschiedenen Zahlen $r - g^{-n'\frac{p-1}{m}}$ erhält, wenn g eine primitive Wurzel von p ist und n' durch die Congruenz $n n' \equiv 1 \pmod{m}$ bestimmt ist.

Nach §. 141 können wir jede ganze oder gebrochene Zahl ω und jedes Functional des Körpers Ω_m in der Weise in Primfactoren zerlegen, dass Zähler und Nenner keinen gemeinschaftlichen Primfactor enthalten, und diese Zerlegung ist, von Einheitsfactoren abgesehen, völlig bestimmt, so dass, wenn $\mathfrak{p}$ ein Primideal ist, ein ganz bestimmter positiver oder negativer Exponent k existirt, so dass das Functional $\omega\,\mathfrak{p}^{-k}$ den Primfactor k weder im Zähler noch im Nenner enthält. Wir sagen dann der Kürze halber, es sei $\mathfrak{p}^k$ die in ω enthaltene Potenz von $\mathfrak{p}$.

Ist $k = 0$, so sagen wir, $\mathfrak{p}$ ist in ω nicht enthalten.

Zwei Zahlen (oder auch Functionale) ω, ω' eines Körpers, in denen ein und dasselbe Primfunctional $\mathfrak{p}$ enthalten ist, wollen wir theilerverwandt oder kurz verwandt nennen; wenn dagegen kein Primfunctional zugleich in ω und in ω' enthalten ist, so heissen ω und ω' theilerfremd oder fremd. Besonders nützlich wird uns dieser Ausdruck in der Folge sein, wenn an

Stelle von ω' die natürliche Primzahl p tritt, die durch $\mathfrak{p}$ theilbar ist, und wir reden danach von den mit einer Zahl ω verwandten oder zu ihr fremden Primzahlen.

Eine Zahl ω, die gar keine verwandten Primzahlen hat, ist eine Einheit.

Im Körper Ω_m (wie überhaupt in jedem Normalkörper) sind alle conjugirten Zahlen ω_n mit denselben Primzahlen verwandt.

§. 174.

Das Kummer'sche Theorem.

Wir haben schon in der Kreistheilungstheorie (Bd. I, §. 169) gewisse Zerlegungen der natürlichen Primzahlen in Factoren, die aus Einheitswurzeln zusammengesetzt waren, kennen gelernt, und es ist nun von Wichtigkeit, zu untersuchen, wie sich diese Factoren zu den Primfactoren im Körper Ω_m verhalten.

Wir betrachten eine Primzahl p, die zum Exponenten 1 gehört, so dass also m ein Theiler von $p - 1$ ist, und setzen

$$p - 1 = m\, m'.$$

Aus den p^{ten} Einheitswurzeln ϱ lassen sich nach Bd. I, §. 167 Perioden von je m' Gliedern bilden, die, wenn g eine primitive Wurzel von p (nicht, wie oben, von m) ist, den Ausdruck haben:

$$(1)\quad \begin{aligned} \eta &= \varrho + \varrho^{g^m} + \varrho^{g^{2m}} + \cdots + \varrho^{g^{(m'-1)m}} \\ \eta_1 &= \varrho^{g} + \varrho^{g^{m+1}} + \varrho^{g^{2m+1}} + \cdots + \varrho^{g^{(m'-1)m+1}} \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_{m-1} &= \varrho^{g^{m-1}} + \varrho^{g^{2m-1}} + \varrho^{g^{3m-1}} + \cdots + \varrho^{g^{p-2}}. \end{aligned}$$

Bezeichnen wir, wie im §. 169 des ersten Bandes, mit ε eine primitive $(p-1)^{\text{te}}$ Einheitswurzel, so dass

$$(2)\qquad \varepsilon^{m'} = r,$$

wie bisher, eine primitive m^{te} Einheitswurzel ist, so sind die Resolventen

$$(3)\qquad (\varepsilon^{\lambda}, \varrho) = \varrho + \varepsilon^{\lambda} \varrho^{g} + \varepsilon^{2\lambda} \varrho^{g^2} + \cdots + \varepsilon^{(p-2)\lambda} \varrho^{g^{p-2}},$$

worin λ jede ganze rationale Zahl sein kann, und speciell für $\lambda = m'$:

$$(4)\qquad (r, \eta) = \eta + r\,\eta_1 + r^2 \eta_2 + \cdots + r^{m-1} \eta_{m-1}.$$

Diese Resolventen sind ganze algebraische Zahlen in gewissen Kreistheilungskörpern, und wir haben, wenn ε^λ nicht $= 1$ ist,

$$(\varepsilon^\lambda, \varrho)\,(\varepsilon^{-\lambda}, \varrho) = (-1)^\lambda\, p,$$

und für $\lambda = m' n$

(5) $$(r^n, \eta)\,(r^{-n}, \eta) = \pm\, p.$$

Es sind also alle diese Resolventen Theiler der natürlichen Primzahl p.

Ausser diesen Resolventen haben wir an der angeführten Stelle noch andere ganze Zahlen der Kreistheilungskörper abgeleitet, nämlich

(6) $$\psi_{\lambda,\mu}(\varepsilon) = \sum_{1,p-2}^{t} \varepsilon^{\mu \operatorname{ind} t - (\lambda+\mu) \operatorname{ind}(t+1)},$$

(worin sich die Indices auf die Basis g beziehen), die im Allgemeinen dem Körper Ω_{p-1} angehören, in dem besonderen Falle, wo λ und μ durch m' theilbar sind, dem Körper Ω_m. Von besonderer Wichtigkeit sind darunter die Zahlen des Körpers Ω_m:

(7) $$\psi_{s m', m'}(\varepsilon) = \psi_s(r) = \sum_{1,p-2}^{t} r^{\operatorname{ind} t - (s+1) \operatorname{ind}(t+1)}.$$

Auch diese Zahlen $\psi_{\lambda,\mu}(\varepsilon)$ sind, wenn keine der Zahlen λ, μ, $\lambda + \mu$ durch $p - 1$ theilbar ist, Theiler von p nach der Formel

$$\psi_{\lambda,\mu}(\varepsilon)\,\psi_{\lambda,\mu}(\varepsilon^{-1}) = p,$$

aus der sich wieder nach (7) ergiebt:

(8) $$\psi_s(r)\,\psi_s(r^{-1}) = p,$$

vorausgesetzt, dass weder s noch $s + 1$ durch m theilbar ist. Gewisse Verbindungen der Resolventen (4), darunter die m^{te} Potenz, haben wir durch die Functionen ψ ausgedrückt [Bd. I, §. 169, (14), (15)]:

(9) $$(r, \eta)^n\,(r^n, \eta)^{-1} = \psi_1(r)\,\psi_2(r) \ldots \psi_{n-1}(r),$$

so lange $n < m$ ist, und

(10) $$(r, \eta)\,(r^{-1}, \eta) = \pm\, p$$

(11) $$(r, \eta)^m = (-1)^{\frac{p-1}{m}}\, p\,\psi_1(r)\,\psi_2(r) \ldots \psi_{m-2}(r),$$

woraus hervorgeht, dass diese m^{ten} Potenzen dem Körper Ω_m angehören.

Wir bezeichnen nun, wie früher, mit $\mathfrak{p}_n$ die verschiedenen Primtheiler von p im Körper Ω_m. Die Zahlen $\psi_s(r)$, die gleichfalls diesem Körper angehören und Factoren von p sind, müssen

daher durch einige dieser Primfactoren theilbar sein, und sie können, so wenig wie p selbst, durch das Quadrat eines $\mathfrak{p}_n$ theilbar sein. Wir müssen feststellen, durch welche Primtheiler $\mathfrak{p}_s$ jede dieser Zahlen $\psi_s(r)$ theilbar ist.

Dazu aber führen einerseits die Congruenzen des vorigen Paragraphen:

$$(12) \qquad r \equiv g^{-n\frac{p-1}{m}} \pmod{\mathfrak{p}_{n'}}, \quad n n' \equiv 1 \pmod{m},$$

andererseits die im §. 170 des ersten Bandes abgeleiteten Congruenzen (17):

$$\begin{aligned} &\psi_{\lambda,\mu}(g) \equiv 0, && \lambda + \mu < p - 1 \\ (13) \qquad &\psi_{\lambda,\mu}(g) \equiv -\frac{\Pi(2p-\lambda-\mu-2)}{\Pi(p-\lambda-1)\,\Pi(p-\mu-1)}, \pmod{p} \\ & && p-1 < \lambda+\mu < 2p-2, \end{aligned}$$

worin λ und μ zwischen 0 und $p-1$ genommen sind, so dass der Binominalcoëfficient

$$\frac{\Pi(2p-\lambda-\mu-2)}{\Pi(p-\lambda-1)\,\Pi(p-\mu-1)}$$

eine durch p nicht theilbare ganze Zahl ist.

Nach der Congruenz (12) ist

$$\psi_s(r) \equiv \psi_s(g^{-nm'}) \equiv \sum^{t} g^{-nm'[\operatorname{ind} t - (s+1)\operatorname{ind}(t+1)]},$$

oder nach (6):

$$\psi_s(r) \equiv \psi_{\lambda,\mu}(g) \pmod{\mathfrak{p}_{n'}},$$

wenn

$$(14) \qquad \begin{matrix} \lambda \text{ den kleinsten positiven Rest von } -nm's \\ \mu \quad " \quad " \quad " \quad " \quad " \quad -nm' \end{matrix} \pmod{p-1}$$

bedeutet, und die Congruenzen (13) zeigen dann, dass $\psi_s(r)$ durch $\mathfrak{p}_{n'}$ theilbar ist, wenn $\lambda + \mu < p - 1$, und nicht theilbar, wenn $\lambda + \mu > p - 1$ ist.

Da die zu m theilerfremde Zahl n nur nach dem Modul m bestimmt ist, so nehmen wir sie jetzt positiv und kleiner als m an. Dann ist

$$\mu = m'(m-n).$$

Die aus (14) bestimmte Zahl λ ist ein Vielfaches von m' und wenn wir $\lambda = m'\varkappa$ setzen, so ist

(15) $\quad \varkappa$ der kleinste positive Rest von $-ns \pmod{m}$.

Hiernach wird $\psi_s(r)$ durch $\mathfrak{p}_{\varkappa'}$ theilbar sein, wenn

$$m'(\varkappa + m - n) < m m'$$

oder $\varkappa < n$, und nicht theilbar, wenn $\varkappa > n$ ist.

Da wir jetzt im Stande sind, für jedes s die Primfactoren von $\psi_s(r)$ zu ermitteln, gehen wir dazu über, die Zahl $(r, \eta)^m$ nach der Formel (11) in ihre Primfactoren zu zerlegen.

Wir bilden zu diesem Zwecke nach (15) die kleinsten positiven Reste $\varkappa$ der Zahlen, $-n, -2n, \cdots -(m-2)n$ nach dem Modul m, und finden, von der Ordnung abgesehen, die Zahlen

$$\varkappa = 1, 2, \ldots, n-1, n+1, \ldots, m-1;$$

die Reste 0 und n kommen darunter nicht vor, weil s keinen Werth erhält, für den s oder $s+1$ durch m theilbar wird. Von diesen Zahlen sind aber gerade $n-1$ kleiner als n, und so oft kommt also der Factor $\mathfrak{p}_{n'}$ in dem Producte $\psi_1 \psi_2 \ldots \psi_{m-2}$ vor. Dann enthält p diesen Factor noch einmal und folglich kommt er nach (11) genau n mal in $(r, \eta)^m$ vor. Da keine anderen als die Primfactoren $\mathfrak{p}_{n'}$ in $(r, \eta)^m$ aufgehen können, so ist hierdurch die Zerlegung vollständig ausgeführt:

$$(16) \qquad (r, \eta)^m = \prod^n \mathfrak{p}_{n'}^n;$$

hierin durchläuft n die Reihe der positiven Zahlen, die kleiner als m und relativ prim zu m sind, und n' ist jedesmal aus der Congruenz

$$(17) \qquad n n' \equiv 1 \pmod m$$

zu bestimmen [1]).

Die Formel (16) gilt für ein gerades wie für ein ungerades m und ist auch noch für den Fall $m = 2$ gültig, für den sie ein schon bekanntes Resultat giebt, da dann $(r, \eta) = (-1, \eta)$ mit einer Gauss'schen Summe übereinstimmt (Bd. I, §. 171).

Wir wollen aber nun, indem wir den Fall $m = 2$ jetzt ausschliessen, der Formel (16) eine etwas allgemeinere Gestalt geben.

Es sei $m = q^\varkappa$ eine beliebige Primzahlpotenz, nur grösser als 2, und p eine von q verschiedene Primzahl von der Eigenschaft, dass $p-1$ durch q oder, wenn $q = 2$ ist, durch 4 theilbar ist.

Es sei ferner m_1 der grösste gemeinschaftliche Theiler von $p-1$ und m, und

$$m = m_1 m_2,$$

---

1) Dieser Satz rührt von Kummer her. Vgl. Theorie der idealen Primfactoren der complexen Zahlen etc. Abhandlungen der Berliner Akademie, 1856.

dann ist nach §. 172, III. die Zerlegung von p in Primfactoren im Körper Ω_m dieselbe, wie im Körper Ω_{m_1}, und es ist

$$\mathfrak{p}_n = \mathfrak{p}_{n+s m_1},$$

wenn s eine beliebige ganze Zahl ist. Wir setzen jetzt

$$t = n + s m_1 \tag{18}$$

und lassen n die Reihe der durch q nicht theilbaren positiven ganzen Zahlen $< m_1$, und s die Zahlenreihe $0, 1, 2, \ldots, m_2 - 1$ durchlaufen, dann durchläuft t ein volles System durch q nicht theilbarer Reste von m, und zwar das ganz bestimmte System, dessen Elemente alle $< m$ sind. Es ist dann nach §. 172

$$p = \prod^{n} \mathfrak{p}_n. \tag{19}$$

Ist ferner t' eine Zahl, die der Congruenz

$$t\,t' \equiv 1 \pmod{m} \tag{20}$$

genügt, so ist, wenn n' durch die Bedingung $n\,n' \equiv 1 \pmod{m_1}$ bestimmt ist,

$$t' \equiv n' \pmod{m_1}. \tag{21}$$

Danach lässt sich das Product

$$\prod^{t} \mathfrak{p}_{t'}^{t}$$

nach der Formel (16) bestimmen, die, auf den Körper Ω_{m_1} angewandt, der aus allen rationalen Functionen der m_1^{ten} Einheitswurzel $r_1 = r^{m_2}$ besteht, die Formel ergiebt:

$$(r_1, \eta)^{m_1} = \prod^{n} \mathfrak{p}_{n'}^{n}. \tag{22}$$

Es ist aber nach (18) und (21)

$$\prod^{t} \mathfrak{p}_{t'}^{t} = \prod^{n} \mathfrak{p}_{n'}^{n m_2} \prod^{n'} \prod^{s} \mathfrak{p}_{n'}^{s m_1},$$

und da n' nach dem Modul m_1 dieselbe Zahlenreihe durchläuft wie n, so ist nach (19):

$$\prod^{s} \prod^{n'} \mathfrak{p}_{n'}^{s m_1} = p^{m_1 \Sigma s} = p^{1/2\, m (m_2 - 1)},$$

und es ergiebt sich:

$$\prod^{t} \mathfrak{p}_{t'}^{t} = [p^{1/2 (m_2 - 1)} (r^{m_2}, \eta)]^{m_1}.$$

Setzen wir

$$\varrho = p^{1/2 (m_2 - 1)} (r_1, \eta), \quad \varrho_n = p^{1/2 (m_2 - 1)} (r_1^n, \eta), \tag{23}$$

so ist ϱ eine Kreistheilungszahl, weil ja auch $\sqrt{p}$ als Werth

einer Gauss'schen Summe zu den Kreistheilungszahlen gehört, und es ist

$$(24) \qquad \varrho^m = \prod^t \mathfrak{p}^t_{t'}.$$

Nach (9) und (11) ist aber, wenn darin m durch m_1 ersetzt wird,

$$(25) \qquad \varrho_n^{m_1} = \pm\, p^{\frac{1}{2} m_1 (m_2 - 1) + 1}\, \psi_1(r_1^n) \ldots \psi_{m_1 - 2}(r_1^n),$$

$$(26) \qquad \varrho^n \varrho_n^{-1} = p^{\frac{1}{2}(n-1)(m_2-1)}\, \psi_1(r_1)\, \psi_2(r_1) \ldots \psi_{n-1}(r_1)$$

und es sind also $\varrho^n \varrho_n^{-1}$, $\varrho_n^{m_1}$ und folglich auch ϱ_n^m Zahlen des Körpers Ω_m, und nach (25) bleibt die in (26) vorkommende Verbindung $\varrho^n \varrho_n^{-1}$ in Ω_m enthalten, wenn n um ein Vielfaches von m_1 vermehrt wird. Es ist demnach $\varrho^n \varrho_n^{-1}$ auch dann noch eine Zahl in Ω_m, wenn n nicht gerade die beschränkte Bedeutung hat wie bisher, sondern eine beliebige durch q nicht theilbare Zahl bedeutet.

Diese Betrachtung hat den Zweck, das Kummer'sche Theorem (16) gleichzeitig auf mehrere verschiedene Primzahlen anwendbar zu machen, die zu verschiedenen Werthen von m_1 gehören, und das Resultat spricht sich dann in folgendem Theorem aus:

3. Es sei φ_n ein System conjugirter Functionale des Körpers Ω_m, das mit keinen anderen natürlichen Primzahlen verwandt ist, als solchen, die nach dem Modul q (oder bei $q = 2$ nach dem Modul 4) mit 1 congruent sind; es durchlaufe ferner t die durch q nicht theilbaren Zahlen der Reihe $1, 2, \ldots, m - 1$, und t' sei aus der Congruenz $t\,t' \equiv 1 \pmod{m}$ bestimmt.

Dann ist das Functional des Körpers Ω_m:

$$\text{a)} \qquad \Phi_n = \prod^t \varphi^t_{n t'} = \varepsilon\, \vartheta_n^m$$

mit der m^{ten} Potenz einer Kreistheilungszahl ϑ_n associirt, die zwar selbst in einem höheren Körper enthalten ist, deren m^{te} Potenz aber dem Körper Ω_m angehört, und es ist

$$\text{b)} \qquad \vartheta_n^{-1}\, \vartheta_1^n = \alpha$$

eine Zahl des Körpers Ω_m.

Der Beweis ist in den vorangegangenen Ausführungen enthalten und ergiebt sich aus den Formeln (25), (26), wenn man

unter ϑ ein Product aus Potenzen der Zahlen ϱ versteht, die nach den Formeln (24) aus den in φ enthaltenen Primfactoren $\mathfrak{p}$ abgeleitet sind.

§. 175.

Die Einheitswurzeln im Körper Ω_m.

Für die weiter zu machenden Anwendungen ist eine genauere Kenntniss der Einheiten des Körpers Ω_m erforderlich, die ja auch an sich von grossem Interesse ist. Wir beschäftigen uns hier nicht mit den functionalen, sondern nur mit den numerischen Einheiten, worunter, wie wir uns erinnern, ganze Zahlen des Körpers Ω_m zu verstehen sind, deren Norm ± 1 ist, oder eine ganze Zahl, deren reciproker Werth gleichfalls ganz ist.

Zu den Einheiten gehören sicher alle in Ω_m enthaltenen Einheitswurzeln; wir können aber leicht beweisen, dass diese Einheitswurzeln nur Potenzen von r sein können, mit positivem und negativem Vorzeichen.

Es sei nämlich ϱ eine in Ω_m enthaltene Einheitswurzel, und

(1) $$\varrho = \varphi(r).$$

Ist q^h die höchste im Grade von ϱ aufgehende Potenz von q, so ist ϱ^{q^h} eine Einheitswurzel, deren Grad nicht durch q theilbar ist, und

(2) $$\varrho^{q^h} = [\varphi(r)]^{q^h}.$$

Wegen der Irreducibilität der Kreistheilungsgleichung im weiteren Sinne [1]) können daher in (2) die sämmtlichen Substitutionen (r, r^n) gemacht werden, ohne dass die linke Seite sich ändert, und folglich ist ϱ^{q^h} eine rationale Zahl, und da es eine Einheit ist, muss es $= \pm 1$ sein. Mithin ist ϱ, vom Vorzeichen abgesehen, einer Einheitswurzel vom Grade q^h oder, wenn $q = 2$ ist, vom Grade q^{h+1} gleich. Es ist nachzuweisen, dass q^h oder q^{h+1} nicht grösser als m sein kann. Dies ergiebt sich aber aus (1). Denn wäre ϱ eine Einheitswurzel höheren als m^{ten} Grades, so wäre r eine Potenz von ϱ, und ϱ müsste einer irreducibeln Gleichung höheren Grades als r, also auch höheren Grades als $\varphi(r)$ genügen, was nach (1) ein Widerspruch ist. Also haben wir den Satz:

[1]) Vgl. Bd. I, §. 134 und den Nachtrag zu diesem Bande.

1. Die einzigen in Ω_m enthaltenen Einheitswurzeln sind die mit positivem und negativem Zeichen genommenen Potenzen von r.

Hieran schliesst sich ein ganz allgemeiner, d. h. in jedem algebraischen Zahlkörper gültiger Satz über die Einheitswurzeln, den wir jetzt beweisen wollen.

Der Satz lautet:

2. Ist α eine ganze Zahl eines algebraischen Zahlkörpers n^{ten} Grades, und haben alle mit α conjugirten Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ den absoluten Werth 1, so ist α eine Einheitswurzel[1]).

Zum Beweis ist zunächst zu bemerken, dass der absolute Werth der Norm einer ganzen Zahl ω dem Product der absoluten Werthe der conjugirten Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ gleich, und als ganze rationale Zahl jedenfalls grösser oder gleich 1 ist. Es ist daher nicht möglich, dass alle diese absoluten Werthe kleiner als 1 sind. Sind sie aber alle gleich 1, wie bei der in unserem Satze angenommenen Zahl α, so muss die Norm $= \pm 1$ sein, und α ist eine Einheit. Ist β eine zweite Einheit, die mit ihren conjugirten zugleich den absoluten Werth 1 hat, so hat der Quotient $\alpha : \beta$ dieselbe Eigenschaft. Wenn daher unter den zu diesem Quotienten conjugirten Zahlen auch nur eine reell ist, so muss

$$\frac{\alpha}{\beta} = \pm 1$$

oder $\alpha = \pm \beta$ sein, und dies gilt dann auch noch, wenn α, β durch die entsprechenden Zahlen eines conjugirten Körpers ersetzt werden.

Wenn also α und β weder gleich noch entgegengesetzt sind, so ist ihr Verhältniss nicht reell, und es besteht daher zwischen den absoluten Werthen die Ungleichung:

$$|\alpha \pm \beta| < |\alpha| + |\beta|.$$

(Vergl. die Einleitung zum ersten Bande, S. 19.)

Es ist also

$$|\alpha \pm \beta| < 2,$$

---

[1]) Kronecker, „Zwei Sätze über Gleichungen mit ganzzahligen Coëfficienten". Crelle's Journal, Bd. 53 (1857). Minkowski, „Geometrie der Zahlen", Art. 43.

und folglich kann $\frac{1}{2}(\alpha \pm \beta)$ keine ganze Zahl sein, weil der absolute Werth der Norm dieser Zahl kleiner als 1 ist. Wenn nun $\omega_1, \omega_2, \ldots, \omega_n$ eine Basis von $\mathfrak{o}$ ist, und

$$\alpha = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$$
$$\beta = b_1\omega_1 + b_2\omega_2 + \cdots + b_n\omega_n,$$

so können die ganzen rationalen Zahlen a, b nicht den Congruenzen

$$a_1 \equiv b_1, \; a_2 \equiv b_2, \ldots, a_n \equiv b_n \pmod 2$$

genügen, weil sonst $\frac{1}{2}(\alpha - \beta)$ eine ganze Zahl wäre.

Wenn wir also die sämmtlichen Zahlen α in 2^n Fächer vertheilen, indem wir alle Zahlen in ein Fach werfen, in denen $a_1, a_2, \ldots, a_n$ dieselben Reste (0 oder 1) nach dem Modul 2 lassen, so können in jedem dieser Fächer höchstens 2 Zahlen, nämlich α und $-\alpha$, vorkommen, und wenn wir $\alpha = 0$ noch ausschliessen, so giebt es sogar in einem dieser Fächer, in dem die $a_1, a_2, \ldots, a_n$ alle gerade sind, gar keine Zahl α. Die Anzahl aller möglichen Zahlen α ist also endlich und höchstens $= 2^{n+1} - 2$.

Wenn nun der absolute Werth von $\alpha = 1$ ist, so gilt dasselbe von allen Potenzen von α. Folglich muss in der unbegrenzten Reihe

$$1, \alpha, \alpha^2, \alpha^3, \ldots$$

nothwendig dieselbe Zahl zum zweiten Male wiederkehren, also $\alpha^h = \alpha^k$ und $k > h$ sein. Dann ist aber

$$\alpha^{k-h} = 1,$$

d. h. α ist eine Einheitswurzel, wie bewiesen werden sollte.

Wir fügen noch die Bemerkung bei, dass, wenn eine Zahl α eines Körpers Ω eine Einheitswurzel m^{ten} Grades ist, auch alle mit α conjugirten Zahlen Einheitswurzeln desselben Grades sind. Denn in der rationalen Gleichung $\alpha^m - 1 = 0$ kann α durch jeden der conjugirten Werthe ersetzt werden.

Die Anzahl der Einheitswurzeln, die in einem Körper Ω enthalten sind, kann immer nur eine endliche sein, weil jede Zahl in Ω einer rationalen Gleichung genügt, deren Grad dem Körpergrad höchstens gleich ist. Der Grad der Einheitswurzeln in Ω kann daher einen endlichen Werth nicht übersteigen.

§. 176.

Der in Ω_m enthaltene reelle Körper H_m.

Jede Zahl des Körpers Ω_m geht durch die Substitution (r, r^{-1}) in die conjugirt imaginäre Zahl über, die auch durch die Vertauschung $(i, -i)$ erhalten wird. Das Product zweier solcher conjugirt imaginärer Zahlen ist das Quadrat des absoluten Werthes einer jeden von ihnen.

Eine Zahl in Ω_m ist reell, wenn sie durch die Vertauschung (r, r^{-1}) ungeändert bleibt, und nur unter dieser Voraussetzung. Jede solche Zahl lässt sich rational durch die zweigliedrige Periode $r + r^{-1}$ ausdrücken, und gehört also einem reellen Körper vom Grade $\frac{1}{2}\varphi(m)$ an, der ein Theiler von Ω_m ist. Diesen wollen wir den in Ω_m enthaltenen reellen Körper nennen und mit H_m bezeichnen (obwohl auch noch andere reelle Körper, nämlich alle Theiler von H_m, in Ω_m enthalten sind).

Die $\frac{1}{2}\varphi(m) = \frac{1}{2}\mu$ Zahlen

(1) $$1,\ r + r^{-1},\ r^2 + r^{-2},\ \ldots,\ r^{\frac{1}{2}\mu - 1} + r^{-\frac{1}{2}\mu + 1}$$

bilden eine Basis der ganzen Zahlen des Körpers H_m. Denn nach §. 170, (7) ist

(2) $$\begin{aligned}\omega = x_0 + x_1 r + x_2 r^2 + \cdots + x_{\frac{1}{2}\mu - 1} r^{\frac{1}{2}\mu - 1} + x_{\frac{1}{2}\mu} r^{\frac{1}{2}\mu} \\ + x_{-1} r^{-1} + x_{-2} r^{-2} + \cdots + x_{-\frac{1}{2}\mu + 1} r^{-\frac{1}{2}\mu + 1}\end{aligned}$$

dann und nur dann eine ganze Zahl des Körpers Ω_m, wenn die Coëfficienten $x_0, x_1, \ldots$ ganze rationale Zahlen sind.

Die Bedingung dafür, dass diese Zahl dem Körper H_m angehört, erhält man, wenn man die Substitution (r, r^{-1}) ausführt und die Differenz $= 0$ setzt. Dividirt man noch durch $r - r^{-1}$, so ergiebt sich so:

$$\begin{aligned}(x_1 - x_{-1}) + (x_2 - x_{-2})(r + r^{-1}) + \cdots \\ + (x_{\frac{1}{2}\mu - 1} - x_{-\frac{1}{2}\mu + 1}) \frac{r^{\frac{1}{2}\mu - 1} - r^{-\frac{1}{2}\mu + 1}}{r - r^{-1}} \\ + x_{\frac{1}{2}\mu} \frac{r^{\frac{1}{2}\mu} - r^{-\frac{1}{2}\mu}}{r - r^{-1}} = 0.\end{aligned}$$

Die Divisionen lassen sich hier ausführen, und wenn man dann mit $r^{\frac{1}{2}\mu - 1}$ multiplicirt, so ergiebt sich für r eine rationale Gleichung von niedrigerem als μ^{ten} Grade, die nur dann be-

friedigt sein kann, wenn alle ihre Coëfficienten verschwinden. Dies führt zu den Gleichungen

$$x_{1/2\mu} = 0,\ x_{1/2\mu-1} = x_{-1/2\mu+1}, \ldots, x_1 = x_{-1},$$

und es ist also jede ganze Zahl ω des Körpers H_m in der Form enthalten:

$$\omega = x_0 + x_1(r + r^{-1}) + x_2(r^2 + r^{-2}) + \cdots \\ + x_{1/2\mu-1}(r^{1/2\mu-1} + r^{-1/2\mu+1}).$$

Statt der Basis (1) kann man auch, wenn man

$$\varrho = r + r^{-1}$$

setzt, die Potenzen von ϱ:

(3) $$1, \varrho, \varrho^2, \ldots, \varrho^{1/2\mu-1}$$

als Basis der ganzen Zahlen von H_m wählen. Denn die Grössen (3) lassen sich ganzzahlig durch die (1) ausdrücken und umgekehrt.

Die Zahl ϱ ist die Wurzel einer irreduciblen Gleichung vom Grade $\frac{1}{2}\mu$, die wir mit $\psi(\varrho) = 0$ bezeichnen wollen. Ist $f(r) = 0$ die Gleichung für r (§. 169), so besteht die identische Relation

(4) $$f(x) = x^{1/2\mu}\,\psi\left(x + \frac{1}{x}\right),$$

woraus durch Bildung der Ableitung

(5) $$f'(r) = r^{1/2\mu}\,\psi'(\varrho)(1 - r^{-2}).$$

Hieraus können wir die Grundzahl Δ_1 des Körpers H_m bilden, die, da H_m nur reelle Zahlen enthält, positiv sein muss. Diese Grundzahl ist, wenn wir die Norm in Bezug auf H_m mit N_1 bezeichnen:

$$\Delta_1 = \pm N_1\,\psi'(\varrho).$$

Ist aber N die in Bezug auf Ω_m gebildete Norm, so ist

$$N\,\psi'(\varrho) = [N_1\,\psi'(\varrho)]^2 = \Delta_1^2,$$

und demnach ergiebt die Formel (5) mit Rücksicht auf §. 169:

$$\Delta = N(1 - r^{-2})\,\Delta_1^2.$$

Nach §. 169, (7) und (10) ist:

$$\begin{aligned} N(1 - r^{-2}) &= q \quad \text{bei ungeradem } q \\ &= 4 \quad \text{für } q = 2, \end{aligned}$$

(6) $$\begin{aligned} \pm\Delta &= q\,\Delta_1^2 \quad \text{bei ungeradem } q \\ &= 4\,\Delta_1^2 \quad \text{für } q = 2. \end{aligned}$$

Setzt man darin

$$\Delta = \pm\, q^{q^{\varkappa-1}[\varkappa(q-1)-1]}$$

so folgt

(7) $$\Delta_1 = q^{\varkappa q^{\varkappa-1}\frac{q-1}{2} - \frac{q^{\varkappa-1}+1}{2}} \quad \text{bei ungeradem } q$$
$$= 2^{(\varkappa-1)2^{\varkappa-2}-1} \quad \text{für } q = 2,$$

so dass Δ_1 immer eine Potenz von q ist.

§. 177.

Die Primideale im Körper H_m.

Es ist jetzt die Frage zu untersuchen, in welcher Beziehung die Primideale des Körpers H_m zu denen des Körpers Ω_m stehen.

Wenn $\mathfrak{P}$ irgend ein Primideal in H_m vom Grade f_1 bedeutet, so muss $\mathfrak{P}$ Theiler einer natürlichen Primzahl p sein, und $\mathfrak{P}$ kann also (nach §. 171) nur dann durch die zweite oder eine höhere Potenz eines Primfactors $\mathfrak{p}$ in Ω_m theilbar sein, wenn $p = q$ ist.

Ist aber $\mathfrak{P}$ ein Theiler von q, so muss es eine Potenz von $\sigma = 1 - r$ sein. Wir setzen etwa

$$\mathfrak{P} = \sigma^\lambda.$$

Nehmen wir hiervon die Norm in Bezug auf Ω_m, die das Quadrat der Norm in Bezug auf H_m ist, so folgt (nach §. 169)

$$q^{2f_1} = q^\lambda,$$

also $f_1 = \frac{1}{2}\lambda$. Da f_1 eine ganze Zahl ist, so muss λ mindestens $= 2$ sein. Es kann aber λ auch nicht grösser als 2 sein, da σ^2 mit der in H_m enthaltenen ganzen Zahl $(1 - r)(1 - r^{-1})$ associirt ist, also σ^2 durch $\mathfrak{P}$ theilbar sein muss. Demnach ist $f_1 = 1$, und wir erhalten den Satz:

1. Die Primzahl q ist die $\frac{1}{2}\mu^{\text{te}}$ Potenz einer in H_m existirenden Primzahl ersten Grades.

Es sei nun p von q verschieden, und $\mathfrak{p}$ ein Primfactor von $\mathfrak{P}$ im Körper Ω_m vom Grade f, der durch die Substitution (r, r^{-1}) in $\mathfrak{p}'$ übergeht. Dann ist $\mathfrak{P}$ sowohl durch $\mathfrak{p}$ als durch $\mathfrak{p}'$ theilbar, und andererseits ist $\mathfrak{p}\mathfrak{p}'$ in H_m enthalten und also durch $\mathfrak{P}$ theilbar, und wir haben zu unterscheiden, ob $\mathfrak{p}$, $\mathfrak{p}'$ verschieden sind oder nicht.

Ist $\mathfrak{p}$ von $\mathfrak{p}'$ verschieden, so ist $\mathfrak{P}$ durch $\mathfrak{p}\mathfrak{p}'$ theilbar, und es folgt $\mathfrak{P} = \mathfrak{p}\mathfrak{p}'$, und durch Normbildung $f_1 = f$.

Ist aber $\mathfrak{p} = \mathfrak{p}'$, so ist $\mathfrak{P} = \mathfrak{p}$, und die Normbildung ergiebt $2 f_1 = f$.

Welcher dieser beiden Fälle eintritt, das hängt also davon ab, ob das Primideal $\mathfrak{p}$ die Substitution (r, r^{-1}) gestattet oder nicht, d. h. ob (r, r^{-1}) in der Gruppe, zu der das Primideal gehört, enthalten ist oder nicht. Nach §. 172 ist dieser Unterschied dadurch bedingt, ob es irgend einen Exponenten h giebt, für den die Congruenz

$$p^h \equiv -1 \pmod{m}$$

erfüllt ist, oder ob es keinen solchen Exponenten giebt.

Wir fassen das Ergebniss folgendermaassen zusammen:

2. Die von q verschiedenen natürlichen Primzahlen p zerfallen in zwei Arten p_1, p_2.

Die erste Art p_1 ist dadurch charakterisirt, dass für irgend einen Exponenten h

$$p_1^h \equiv -1 \pmod{m},$$

und diese Primzahlen zerfallen, wenn sie für den Modul m zum Exponenten f gehören und $\mu = ef$ gesetzt wird, im Körper H_m in e Primfactoren $\frac{1}{2} f^{\text{ten}}$ Grades. Ihre Primfactoren sind auch in Ω_m nicht weiter zerlegbar.

Die Primzahlen der zweiten Art p_2 sind dadurch bestimmt, dass keine ihrer Potenzen nach dem Modul m mit -1 congruent wird, und sie zerfallen im Körper H_m in $\frac{1}{2} e$ Primfactoren f^{ten} Grades. Ihre Primfactoren sind in Ω_m noch in je zwei Factoren zerlegbar.

Bei den Primzahlen der ersten Art muss f sicher eine gerade Zahl sein. Wenn m ungerade ist, so genügt es auch, damit p eine Primzahl von der ersten Art sei, dass sie zu einem geraden Exponenten gehöre; denn dann ist

$$(p^{1/2 f} - 1)(p^{1/2 f} + 1) \equiv 0 \pmod{m}.$$

Der erste dieser Factoren $p^{1/2 f} - 1$ ist aber nicht durch m theilbar, weil sonst p zum Exponenten $\frac{1}{2} f$ gehören würde. Folglich muss $p^{1/2 f} + 1$ durch q theilbar sein. Hier können aber nicht beide Factoren $p^{1/2 f} - 1$ und $p^{1/2 f} + 1$ durch q theilbar sein, weil sonst auch ihre Differenz, die $= 2$ ist, durch q theilbar wäre, und folglich ist $p^{1/2 f} + 1$ durch m theilbar.

Ist aber m eine Potenz von 2, so ist die Congruenz

$$p^h \equiv -1 \pmod{m}$$

nur dann möglich, wenn $p \equiv -1 \pmod{m}$ ist. Denn jede gerade Potenz einer ungeraden Zahl ist $\equiv +1 \pmod{8}$ und kann also nicht $\equiv -1 \pmod{m}$ sein. Ist aber h ungerade, so ist

$$\frac{p^h + 1}{p + 1} = p^{h-1} - p^{h-2} + \cdots + 1$$

selbst ungerade, und folglich ist $p^h + 1$ durch keine höhere Potenz von 2 theilbar, als $p + 1$. Demnach können wir dem Satze 2. noch folgende nähere Bestimmung hinzufügen:

3. Wenn m ungerade ist, so gehören die Primzahlen p_1 zu einem geraden, die Primzahlen p_2 zu einem ungeraden Exponenten.

   Ist m gerade, so gehören die Primzahlen der Form $km - 1$ zur ersten und alle anderen ungeraden Primzahlen zur zweiten Art.

§. 178.

Die Einheiten des Körpers H_m.

Die dem Körper H_m angehörigen Einheiten sind von besonderer Wichtigkeit für die Anwendungen. Auf sie lassen sich auch die Einheiten des Körpers Ω_m zurückführen nach folgendem Satze:

1. Jede Einheit des Körpers Ω_m ist das Product einer Einheitswurzel und einer reellen Einheit des Körpers Ω_m.

Bezeichnen wir irgend eine Einheit des Körpers Ω_m mit $\mathfrak{E}(r)$, so ist $\mathfrak{E}(r^{-1})$ der conjugirt imaginäre Werth, der gleichfalls eine Einheit darstellt, und der Quotient $\mathfrak{E}(r) : \mathfrak{E}(r^{-1})$ ist wieder eine Einheit, deren absoluter Werth

$$(1) \qquad \sqrt{\frac{\mathfrak{E}(r)}{\mathfrak{E}(r^{-1})} \frac{\mathfrak{E}(r^{-1})}{\mathfrak{E}(r)}}$$

gleich 1 ist, und folglich ist dieser Quotient eine Einheitswurzel und mithin $= \pm r^h$, worin h irgend ein ganzzahliger Exponent ist (§. 175, Satz 1., 2.). Wir haben also

$$(2) \qquad \mathfrak{E}(r) = \pm r^h \, \mathfrak{E}(r^{-1}).$$

Es ist nun im weiteren Beweise ein kleiner Unterschied zu machen, je nachdem m ungerade oder gerade ist.

Ist m zunächst ungerade, so können wir in (2) den Exponenten h gerade annehmen, da wir ihn nöthigenfalls durch $h + m$ ersetzen können. Ferner ist in der Formel (2) nur das obere Zeichen zulässig. Denn wenn das untere Zeichen stände, so würde folgen:

$$\mathfrak{E}(r) \equiv \mathfrak{E}(1) \equiv -\mathfrak{E}(1), \quad 2\mathfrak{E}(1) \equiv 0 \; [\mathrm{mod}\,(1-r)].$$

Nach §. 169 ist aber $1 - r$ ein Theiler von q, also relativ prim zu 2, und daher ist $\mathfrak{E}(1)$ und folglich auch $\mathfrak{E}(r)$ durch $(1 - r)$ theilbar. Dies aber widerspricht der Voraussetzung, dass $\mathfrak{E}(r)$ eine Einheit sein soll.

Demnach ergiebt sich aus (2):

$$r^{-\frac{1}{2}h}\,\mathfrak{E}(r) = r^{\frac{1}{2}h}\,\mathfrak{E}(r^{-1}),$$

woraus folgt, dass $r^{-\frac{1}{2}h}\,\mathfrak{E}(r)$ eine reelle Einheit ist. Bezeichnen wir sie mit $e(r)$, so ist also

(3) $$\mathfrak{E}(r) = r^{\frac{1}{2}h}\,e(r),$$

woraus für diesen Fall das Theorem 1. bewiesen ist.

Wenn aber zweitens m eine Potenz von 2 ist, so ist $\mu = \frac{1}{2}m$ und $r^{\mu} = -1$, und zugleich mit r ist $-r$ eine m^{te} Einheitswurzel. Wenn wir nöthigenfalls h durch $h + \frac{1}{2}m$ ersetzen, so können wir in (2) das obere Zeichen annehmen und setzen:

(4) $$\mathfrak{E}(r) = r^{h}\,\mathfrak{E}(r^{-1}).$$

Es kommt jetzt darauf an, nachzuweisen, dass h gerade sein muss.

Wenn wir $\mathfrak{E}(r)$ durch die Basis $1, r, r^2, \ldots r^{\mu-1}$ darstellen, so ergiebt sich

(5) $$\mathfrak{E}(r) = \sum_{0,\,\mu-1}^{s} x_s r^s,$$

worin die x_s ganze rationale Zahlen sind. Nach (4) ist aber dann

$$\sum_{0,\,\mu-1}^{s} x_s r^s = \sum_{1,\,\mu-1}^{s} x_s r^{h-s},$$

und daraus folgt, dass $x_s = \pm x_{s'}$ ist, wenn $s + s' \equiv h \pmod{\mu}$. Ist nun h ungerade, so ist aus zwei so verbundenen Zahlen die eine gerade, die andere ungerade (da μ eine Potenz von 2 ist). Der Ausdruck (5) ergiebt also für $\mathfrak{E}(r)$ ein Aggregat von Gliedern der Form

$$x_s(r^s \pm r^{s'}).$$

Es ist aber $r^s \pm r^{s'} = r^s(1 \pm r^{h-2s}) = r^s(1 \mp r^{\mu+h-2s})$ immer durch $1 - r$ theilbar, und daraus würde folgen, dass $\mathfrak{E}(r)$ durch $1 - r$, was keine Einheit ist, theilbar wäre, was dem Begriffe der Einheit widerspricht. Also ist die Annahme unzulässig, dass in der Formel (4) der Exponent h ungerade sei, und wir können wie oben

$$\mathfrak{E}(r) = r^{1/2 h} e(r)$$

setzen, worin $e(r)$ eine reelle Einheit ist. Damit ist der Satz 1. bewiesen.

Wir wollen ein System von reellen Einheiten hervorheben: Nach §. 169 sind die μ Grössen $1 - r^n$ alle unter einander associirt. Demnach ist der Quotient

$$\frac{1 - r^n}{1 - r^{n'}},$$

worin n, n' zwei relative Primzahlen zu m bedeuten, eine Einheit. Daraus leitet man aber, wenn

$$r = e^{\frac{2\pi i}{m}}$$

gesetzt wird, die reelle Einheit

$$(6) \qquad \frac{\sin \frac{n\pi}{m}}{\sin \frac{n'\pi}{m}} = \frac{r^{\frac{n}{2}} - r^{-\frac{n}{2}}}{r^{\frac{n'}{2}} - r^{-\frac{n'}{2}}} = r^{\frac{n'-n}{2}} \frac{1 - r^n}{1 - r^{n'}}$$

her. Ist m gerade, so kann man $n' = n + \frac{m}{2}$ setzen, und erhält für diesen Fall die reellen Einheiten

$$(7) \qquad \tau_n = \operatorname{tang} \frac{n\pi}{m},$$

worin n jede ungerade Zahl bedeuten kann.

Ersetzt man n durch $\frac{1}{2}m - n$, so geht τ_n in den reciproken Werth über. Lässt man n die Reihe der Zahlen

$$1, 3, 5, \cdots, \frac{m}{4} - 1$$

durchlaufen, so erhält τ_n lauter positive echt gebrochene Werthe.

Zweiundzwanzigster Abschnitt.

Abel'sche Körper und Kreistheilungskörper.

---

§. 179.

Einfache Abel'sche Körper.

Wir wenden uns nun zu einer der interessantesten Anwendungen der Theorie der algebraischen Zahlen.

Es handelt sich um den Beweis des allgemeinen Satzes[1]):

I. **Alle im absoluten Rationalitätsbereich Abel'schen Zahlkörper sind Kreistheilungskörper.**

Haben wir diesen Satz bewiesen, so gewinnen die Untersuchungen des dritten Abschnittes über Kreistheilungskörper ein erhöhtes Interesse, weil damit gezeigt ist, dass auf dem dort angegebenen Wege nicht nur alle Kreistheilungskörper, sondern alle Abel'schen Körper überhaupt gefunden werden.

Es sei $\Omega = R(x)$ ein Abel'scher Körper m^{ten} Grades, d. h. ein Körper, der aus allen rationalen Functionen einer Wurzel x einer irreduciblen Abel'schen Gleichung m^{ten} Grades besteht, wenn als Rationalitätsbereich der Körper R der rationalen Zahlen betrachtet wird. Die Galois'sche Gruppe $\mathfrak{G}$ dieser Gleichung, die also eine Abel'sche Gruppe ist und denselben Grad m hat, wie der Körper Ω, ist auch die Gruppe des Körpers Ω.

Ist x_1 eine nicht primitive Zahl aus Ω, so ist $\Omega_1 = R(x_1)$ gleichfalls ein Abel'scher Körper, den wir einen echten Theiler von Ω nennen und dessen Grad ein echter Theiler des Grades von Ω ist. Denn ist $\mathfrak{A}$ die Gruppe, zu der die Zahl x_1 gehört,

---

[1]) Kronecker hat diesen Satz zuerst ausgesprochen, aber keinen vollständigen Beweis dafür veröffentlicht. Den ersten Beweis hat der Verfasser des vorliegenden Werkes in Bd. 8 der Acta Mathematica bekannt gemacht (1886). In neuester Zeit ist ein zweiter Beweis von Hilbert veröffentlicht, der sich auf die im neunzehnten Abschnitte entwickelten Sätze stützt (Nachrichten d. Gesellschaft d. Wissenschaften zu Göttingen, 1896, Heft 1).

so ist $\mathfrak{G} | \mathfrak{A}$ (§. 4 dieses Bandes) die Gruppe des Körpers Ω_1 und dies ist zugleich mit $\mathfrak{G}$ eine Abel'sche Gruppe. Ein Theiler von Ω, der mit Ω von gleichem Grade ist, ist mit Ω identisch (vgl. Bd. I, §. 144, 149, 156).

Giebt es nun zwei nicht primitive Zahlen x_1, x_2 in Ω von der Art, dass

$$\Omega = R\,(x_1, x_2)$$

gesetzt werden kann, so sind die Körper $\Omega_1 = R(x_1)$, $\Omega_2 = R(x_2)$ echte Theiler von Ω, und Ω heisst aus den beiden Körpern Ω_1, Ω_2 zusammengesetzt.

Gestattet der Körper Ω keine solche Darstellung, so heisst er einfach.

Wenn also als bewiesen vorausgesetzt wird, dass Ω_1, Ω_2 Kreistheilungskörper sind, d. h. dass alle ihre Zahlen rational durch Einheitswurzeln darstellbar sind, so folgt dasselbe für Ω.

Wenn einer der Körper Ω_1, Ω_2 zerlegbar ist, so können wir die Zerlegung wiederholen, und müssen, da die Grade abnehmende ganze positive Zahlen sind, endlich zu einfachen Körpern gelangen.

Das Theorem I. braucht also nur für einfache Abel'sche Körper bewiesen zu werden.

Es ist aber daran zu erinnern, dass die Zerlegbarkeit eines Körpers Ω keineswegs schon aus der Existenz eines Theilers folgt, und dass bei einem zerlegbaren Körper die Zerlegung in einfache Körper auf ganz verschiedene Arten geschehen kann, so dass bei den Körpern nicht die Gesetze der Theilbarkeit gelten, wie im Gebiete der Zahlen.

Ein Kennzeichen für die Einfachheit eines Körpers können wir aus seiner Gruppe ableiten.

Wenn die Gruppe $\mathfrak{G}$ zwei echte Theiler $\mathfrak{A}$ und $\mathfrak{B}$ von der Art hat, dass jedes Element ein- und nur einmal aus einem Element von $\mathfrak{A}$ und einem Element von $\mathfrak{B}$ zusammengesetzt werden kann, so nennen wir die Gruppe $\mathfrak{G}$ zerlegbar in die beiden Componenten $\mathfrak{A}, \mathfrak{B}$; $\mathfrak{G}$ ist also zerlegbar, wenn in dem nach der Composition der Theile (§. 4) gebildeten Producte

$$\mathfrak{G} = \mathfrak{A}\,\mathfrak{B} \tag{1}$$

jedes Element von $\mathfrak{G}$ ein- und nur einmal erscheint. Der Grad von $\mathfrak{G}$ ist dann gleich dem Producte der Grade von $\mathfrak{A}$ und $\mathfrak{B}$.

Giebt es solche Theiler nicht, so heisst die Gruppe $\mathfrak{G}$ unzerlegbar.

Dann können wir den Satz beweisen:

1. **Ist die Gruppe eines Abel'schen Körpers zerlegbar, so ist auch der Körper zusammengesetzt.**

Nehmen wir, um dies zu beweisen, an, die Gruppe $\mathfrak{G}$ des Körpers Ω sei nach der Formel (1) zerlegbar und m, a, b seien die Grade von $\mathfrak{G}, \mathfrak{A}, \mathfrak{B}$. Wir nehmen eine zur Gruppe $\mathfrak{B}$ gehörige Zahl ξ des Körpers Ω, die also durch die Substitutionen von $\mathfrak{G}$ in a verschiedene conjugirte Werthe übergeht und ebenso eine zu $\mathfrak{A}$ gehörige b-werthige Zahl η. Wir können dann eine Zahl

$$x = \alpha\xi + \beta\eta$$

mit rationalen Zahlencoëfficienten α, β bilden, die m verschiedene conjugirte Werthe hat, und dann ist $\Omega = R(x)$. Also ist Ω aus $R(\xi)$ und $R(\eta)$ zusammengesetzt (Bd. I, §. 143).

Erinnern wir uns nun an die in §. 9, 10 dieses Bandes abgeleitete Darstellung einer Abel'schen Gruppe durch eine Basis, so ergiebt sich durch wiederholte Anwendung des eben Bewiesenen:

2. **Jeder Abel'sche Körper Ω lässt sich aus solchen zusammensetzen, deren Grad eine Primzahlpotenz und deren Gruppe cyklisch ist. Die Grade dieser zusammensetzenden Körper sind die Invarianten der Gruppe von Ω.**

Diese Sätze werden durch den folgenden ergänzt:

3. Ein Abel'scher Körper von Primzahlpotenzgrad mit cyklischer Gruppe ist einfach.

Wenn die Gruppe $\mathfrak{G}$ cyklisch ist, so lassen sich ihre Elemente durch die Potenzen einer Basis, G^γ, darstellen, wenn γ ein volles Restsystem nach dem Modul m durchläuft. Wir erhalten alle Theiler $\mathfrak{A}$ von $\mathfrak{G}$ dargestellt durch

$$\mathfrak{A} = G^{b\gamma},$$

wenn b ein Theiler von m ist und γ ein volles Restsystem nach dem Modul $a = m : b$ durchläuft.

Ist

$$\mathfrak{A}' = G^{b'\gamma}$$

ein zweiter Theiler von $\mathfrak{G}$ vom Grade a' und ist

$$b' \gtreqless b, \quad a' \lesseqgtr a,$$

so ist, wenn wir jetzt annehmen, dass m und mithin auch a, b, a', b' Potenzen einer Primzahl q sind, b' ein Theiler von b und folglich $\mathfrak{A}$ ein Theiler von $\mathfrak{A}'$.

Wenn also ξ eine Zahl des Körpers Ω ist, die zu der Gruppe $\mathfrak{A}$ gehört, so ist ξ eine primitive Zahl des Körpers b^{ten} Grades $R(\xi)$, und in diesem Körper ist auch jede Zahl ξ' enthalten, die die Substitutionen der Gruppe $\mathfrak{A}'$ gestattet. Sind also $\mathfrak{A}, \mathfrak{B}$ und $\mathfrak{A}', \mathfrak{B}'$ echte Theiler von $\mathfrak{G}$, so ist $R(\xi)$ von Ω verschieden, und $R(\xi)$ wird durch Adjunction von ξ' nicht erweitert. Es kann also auch nicht Ω aus $R(\xi)$ und $R(\xi')$ zusammengesetzt werden, wodurch 3. bewiesen ist.

§. 180.

Die Resolventen.

Nach dem, was jetzt bewiesen ist, können wir uns in den weiteren Betrachtungen, die den Beweis des Satzes I. zum Ziele haben, auf solche Abel'sche Körper beschränken, deren Grad eine Primzahlpotenz und deren Gruppe cyklisch ist. Aus diesem Grunde genügte es auch für die beabsichtigte Anwendung, dass wir im vorigen Abschnitte uns auf die Betrachtung der Kreistheilungskörper Ω_m beschränkt haben, in denen m eine Primzahlpotenz war. Wir behalten so viel als möglich die dort gebrauchte Bezeichnung bei und setzen

(1) $$m = q^{\varkappa},$$

worin q eine Primzahl, $\varkappa$ ein positiver Exponent ist, und in dem Falle, dass $q = 2$ ist, nehmen wir $\varkappa > 1$ an. Mit n bezeichnen wir jede durch q nicht theilbare Zahl. Es ist r eine primitive m^{te} Einheitswurzel und Ω_m der Körper der rationalen Functionen von r.

Es sei nun $\Omega = R(x)$ ein einfacher Abel'scher Körper m^{ten} Grades, so dass x Wurzel einer rationalen irreduciblen cyklischen Gleichung m^{ten} Grades ist. Bezeichnen wir die Wurzeln dieser Gleichung in geeigneter Reihenfolge mit

(2) $$x_0, x_1, x_2, \ldots, x_{m-1},$$

und nehmen $x_m = x_0, x_{m+1} = x_1, \ldots$ an, so ist

$$x_1 = \Phi(x_0),\ x_2 = \Phi(x_1), \ldots, x_0 = \Phi(x_{m-1}),$$

worin Φ eine ganze Function mit rationalen Coëfficienten bedeutet, und die Gruppe des Körpers Ω besteht aus den Potenzen der Substitution (x_0, x_1) oder aus den cyklischen Permutationen

der Wurzeln (2). Jede cyklische Function dieser Grössen ist eine rationale Zahl. Was wir zu beweisen haben, ist, dass sich die x rational durch Einheitswurzeln ausdrücken lassen. Adjungiren wir dem Körper Ω noch die m^{te} Einheitswurzel r, so entsteht ein Körper $R(x, r)$, der die beiden Körper $\Omega = R(x)$ und $R(r) = \Omega_m$ als Theiler enthält.

Wenn eine Zahl $\omega = \Phi(x, r)$ des Körpers $R(x, r)$ die sämmtlichen Substitutionen $(x_0, x_1), (x_0, x_2), \ldots, (x_0, x_{m-1})$ gestattet, so ist sie im Körper Ω_m enthalten; denn dann ist

$$m\omega = \Phi(x_0, r) + \Phi(x_1, r) + \cdots + \Phi(x_{m-1}, r),$$

und darin sind die Coëfficienten der Potenzen von r nicht nur cyklische, sondern sogar symmetrische Functionen der Wurzeln (2), also rationale Zahlen. Dies gilt selbst noch in dem Falle, dass die Gleichung für x durch Adjunction von r reducirt wird.

Dies wenden wir an auf die Resolventen

(3) $$(r, x_0) = x_0 + r x_1 + r^2 x_2 + \cdots + r^{m-1} x_{m-1},$$

und allgemeiner, wenn s einen beliebigen ganzzahligen Exponenten bedeutet:

(4) $$(r^s, x_0) = x_0 + r^s x_1 + r^{2s} x_2 + \cdots + r^{(m-1)s} x_{m-1}.$$

Durch diese Resolventen lässt sich x_0 selbst wieder rational ausdrücken, nämlich:

(5) $$m x_0 = \sum_{0, m-1}^{s} (r^s, x_0),$$

und wenn wir also nachweisen können, dass alle diese Resolventen (r^s, x_0) Kreistheilungszahlen sind, so haben wir unser Ziel erreicht. Wenn wir

(6) $$(r^s, x_\varkappa) = x_\varkappa + r^s x_{\varkappa+1} + r^{2s} x_{\varkappa+2} + \cdots + r^{(m-1)s} x_{\varkappa+m-1}$$

setzen, so geht $(r^s, x_\varkappa)$ aus (r^s, x_0) durch die Substitution $(x_0, x_\varkappa)$ hervor, und es besteht die fundamentale Relation

(7) $$r^{\varkappa s} (r^s, x_\varkappa) = (r^s, x_0).$$

Alle diese Resolventen sind Zahlen des Körpers $R(x, r)$; wir betrachten vorzugsweise die beiden folgenden Verbindungen:

(8) $$(r^s, x_0)^m = \omega_s,$$

(9) $$(r^s, x_0)^{-1} (r, x_0)^s = \alpha.$$

Diese beiden Zahlen gestatten, wie aus (7) unmittelbar hervorgeht, die Substitutionen $(x_0, x_\varkappa)$, und sind also Zahlen des Körpers Ω_m.

Ist n durch q nicht theilbar, so kann wegen der Irreducibilität der Kreistheilungsgleichung keine von den Resolventen (r^n, x_0) verschwinden, wenn sie nicht alle verschwinden; denn die Gleichung

$$(r, x_0)^m = 0$$

wäre eine Gleichung für r mit rationalen Coëfficienten, die alle Substitutionen (r, r^n) gestattet.

Ebenso kann keine der Resolventen (r^s, x_0) verschwinden, wenn nicht die ganze Schaar verschwindet, in der s einen bestimmten grössten gemeinschaftlichen Theiler mit m hat.

Wenn alle (r, x_0) verschwinden, so ist die Formel (9) nicht anwendbar. Dann können wir aber die Resolventen (r^q, x_0) direct betrachten, die zu einem Körper vom Grade $m\,q^{-1}$ gehören, der aus

$$y_0 = x_0 + x_q + x_{2q} + \cdots + x_{m-q}$$

hervorgeht, und wenn auch diese Grössen verschwinden, so gehen wir zu den Resolventen (r^{q^2}, x_0) über u. s. f.

Wenn aber (r, x_0) nicht verschwindet, so lassen sich durch die Formel (9) alle (r^s, x_0) rational durch (r, x_0) und durch Kreistheilungszahlen darstellen.

Demnach ist es für unseren Zweck ausreichend, wenn wir beweisen können, dass die nicht verschwindenden Resolventen (r, x_0) Kreistheilungszahlen sind.

Lassen wir n ein volles System incongruenter, durch q nicht theilbarer Zahlen durchlaufen, so ist

$$\sum n \equiv 0 \pmod{m},$$

denn die Zahlen n zerfallen in Paare einander zu m ergänzender Zahlen. Daraus folgt nach (7), dass das Product

$$(10) \qquad \prod^{n} (r^n, x_0) = a$$

eine Zahl in Ω_m ist. Da aber diese Zahl sich überdies nicht ändert, wenn irgend eine der Substitutionen (r, r^n) darin ausgeführt wird, so ist a eine rationale Zahl.

§. 181.

Vorbereitung zum Beweis.

Nach den Ausführungen des vorigen Paragraphen ist zum Beweis des grossen Theorems I nur noch der Nachweis erforderlich, dass die in Ω_m enthaltene Zahl

$$\omega = (r, x_0)^m$$

die m^{te} Potenz einer Kreistheilungszahl ist.

1. **Die wesentliche Eigenschaft der zu ω conjugirten Zahlen ω_n, auf die sich der Beweis stützt, ist die, dass**

(1) $$\omega_n^{-1}\,\omega_1^n = \alpha^m$$

die m^{te} Potenz einer Zahl in Ω_m ist.

Hierin kann n jede durch q nicht theilbare Zahl sein. Bilden wir von der rechten und linken Seite von (1) die Normen im Körper Ω_m, so ergiebt sich, wenn wir die Norm der Zahl α, die eine rationale Zahl ist, mit a bezeichnen, da jedes ω_n dieselbe Norm wie ω hat,

$$N(\omega)^{n-1} = a^m.$$

Wenn nun m ungerade ist, so können wir hierin $n = 2$ annehmen, und erhalten als Folgerung aus 1.:

2. **Die Norm von ω ist die m^{te} Potenz einer rationalen Zahl**

(2) $$N(\omega) = a^m.$$

Ist m eine Potenz von 2., so ist diese Folgerung nicht mehr zulässig. Es ergiebt sich dann aus 1. nur, dass $N(\omega)^2$ die m^{te} Potenz einer rationalen Zahl ist. Gleichwohl müssen die Zahlen ω, wie aus (10) des vorigen Paragraphen zu sehen ist, auch in diesem Falle noch der Bedingung 2. genügen, die dann aber nicht mehr von selbst schon in 1. enthalten ist, sondern als neue Eigenschaft hinzukommt.

Was wir zu beweisen haben, ist, dass aus 1. und 2. folgt, dass auch ω selbst die m^{te} Potenz einer Kreistheilungszahl, wenn auch in einem höheren Körper, ist.

Dazu ist aber erforderlich, die Zerlegung der Zahlen ω in ihre Primfactoren im Körper Ω_m zu untersuchen.

Die Primzahl q ist, wie im §. 169 nachgewiesen, mit der $\varphi(m)^{ten}$ Potenz einer in Ω_m existirenden Primzahl $\sigma = 1 - r$

associirt. Ist also σ^k die in ω enthaltene Potenz von σ, so setzen wir

$$\omega = \sigma^k \omega',$$

worin ω' mit der Primzahl q theilerfremd ist. Die Bildung der Norm ergiebt nach 2.

$$a^m = q^k b,$$

worin b eine rationale Zahl ist, die in einfachster Gestalt die Primzahl q weder im Zähler noch im Nenner enthält. Daraus ergiebt sich aber, dass k durch m theilbar sein muss, und daraus das erste Resultat:

3. Der Exponent der in ω enthaltenen Primzahl σ ist immer durch m theilbar.

Es sei nun ferner p eine von q verschiedene Primzahl und $\mathfrak{p}_\xi$ ein Primfactor von p im Körper Ω_m. Wir lassen ξ die im §. 172 in den verschiedenen Fällen näher bestimmte Zahlenreihe $\xi_1, \xi_2, \ldots, \xi_e$ durchlaufen, so dass

(3) $$p = \mathfrak{p}_{\xi_1} \mathfrak{p}_{\xi_2} \ldots \mathfrak{p}_{\xi_e}$$

wird, und nehmen an, es sei $\mathfrak{p}_\xi^{k_\xi}$ die in ω enthaltene Potenz von $\mathfrak{p}_\xi$. Die in ω_n enthaltene Potenz von $\mathfrak{p}_{n\xi}$ ist dann $\mathfrak{p}_{n\xi}^{k_\xi}$, und wenn wir n' aus der Congruenz

(4) $$n\, n' \equiv 1 \pmod{m}$$

bestimmen, so ist $\mathfrak{p}_\xi^{k_{n'\xi}}$ die in ω_n enthaltene Potenz von $\mathfrak{p}_\xi$. Demnach ist in

(5) $$\omega_n^{-1} \omega_1^n \text{ die Potenz } \mathfrak{p}_\xi^{n k_\xi - k_{n'\xi}}$$

enthalten, und wegen 1. muss der Exponent dieser Potenz durch m theilbar sein.

Wir erhalten also für jedes durch q nicht theilbare n die Congruenz

(6) $$n\, k_\xi \equiv k_{n'\xi} \pmod{m},$$

in der wir nun auch ξ durch $n\xi$ ersetzen können, wodurch sich

(7) $$n\, k_{n\xi} \equiv k_\xi \pmod{m}$$

ergiebt. Nehmen wir hierin $\xi = 1$ und setzen dann ξ, ξ' für n, n' und k für k_1, so folgt aus (7)

(8) $$k_\xi \equiv \xi' k \pmod{m},$$

worin nun k für alle ξ denselben Werth hat und ξ, ξ' durch die Congruenz

$$\xi\, \xi' \equiv 1 \pmod{m}$$

zusammenhängen.

Nehmen wir $n = p$ an, so wird $\mathfrak{p}_{p\xi} = \mathfrak{p}_{\xi}$ (§. 172), also ist auch $k_{p\xi} = k_{\xi}$, und aus (7) und (8) folgt:

(9) $$k\,(p - 1) \equiv 0 \pmod{m}.$$

Hieraus ergeben sich nun wichtige Folgerungen: Wenn zunächst $p - 1$ nicht durch q theilbar ist, so folgt, dass k durch m theilbar sein muss, und wir haben also den Satz:

4. Die Primfactoren einer Primzahl p, die nach dem Modul q nicht mit 1 congruent ist, sind in ω nur in solchen Potenzen enthalten, deren Exponenten durch m theilbar sind.

Wenn in dem Falle, wo m eine Potenz von 2 ist, $p - 1$ durch 2, aber nicht durch 4 theilbar ist, wenn also $p \equiv -1 \pmod{4}$ ist, so folgt aus (9) nur, dass k durch $\frac{1}{2}m$, nicht aber, dass k durch m theilbar ist. Der Exponent der in ω enthaltenen Potenz von $\mathfrak{p}_{\xi}$ ist, von Vielfachen von m abgesehen, gleich k, und wenn k durch m theilbar ist, so ist alles wie im Falle 4. Ist aber k nur durch $\frac{1}{2}m$, nicht durch m theilbar, also

$$k \equiv \tfrac{1}{2}m \pmod{m},$$

so ist $k - \frac{1}{2}m$ durch m theilbar, und wir können mit Rücksicht auf die Zerlegung (3) den Satz so formuliren:

5. Ist m eine Potenz von 2 und p eine Primzahl congruent mit -1 nach dem Modul 4, so lässt sich der Exponent h so bestimmen, dass alle Primfactoren von p in

$$\omega\,\sqrt{p}^{\,-hm}$$

nur zu solchen Potenzen enthalten sind, deren Exponent durch m theilbar ist.

Es sei endlich $p - 1$ durch q, oder, falls m gerade ist, durch 4 theilbar. Ist m_1 der grösste gemeinschaftliche Theiler von m und $p - 1$, und ist

$$m = m_1\, m_2,$$

so muss k nach (9) durch m_2 theilbar sein, und wenn wir

$$k = h\, m_2$$

setzen, so ist in ω nach (8) das Product enthalten:

(10) $$\Bigl(\prod^{\xi} \mathfrak{p}_{\xi}^{\xi'}\Bigr)^{h m_2}.$$

Ausserdem kommen in ω die Primfactoren $\mathfrak{p}_{\xi}$ nur noch in solchen Potenzen vor, deren Exponenten durch m theilbar sind.

In diesem Falle durchläuft nun ξ nach §. 172, III ein volles System durch q nicht theilbarer Reste nach dem Modul m_1, und wir können in (10) unter ξ' die kleinste positive Lösung der Congruenz

$$\xi\, \xi' \equiv 1 \pmod{m_1}$$

verstehen, weil, wenn wir die Exponenten ξ' in (10) nach dem Modul m_1 verändern, nur m^{te} Potenzen der Primfactoren $\mathfrak{p}$ hinzutreten.

Dann können wir auf das Product (10) das Kummer'sche Theorem [§. 174, (16)] anwenden, indem wir dort m durch m_1 ersetzen, und erhalten, wenn wir unter $r_1 = r^{m_2}$ eine m_1^{te} Einheitswurzel, unter den η gewisse Perioden der p^{ten} Einheitswurzeln verstehen:

$$\prod^{\xi} \mathfrak{p}_{\xi}^{\xi'} = (r_1, \eta)^{m_1},$$

und folglich

$$(11) \qquad \left(\prod^{\xi} \mathfrak{p}_{\xi}^{\xi'}\right)^{h m_2} = (r_1, \eta)^{h m}.$$

Demnach haben wir das Theorem:

6. Ist p eine Primzahl und $p - 1$ durch q, oder, wenn $q = 2$ ist, durch 4 theilbar, so lässt sich der positive Exponent h so bestimmen, dass die in Ω_m enthaltene Zahl

$$\omega\, (r_1, \eta)^{-h m}$$

die Primfactoren von p nur zu solchen Potenzen enthält, deren Exponent durch m theilbar ist.

Es ist jetzt auch nicht mehr nöthig, den Satz 5. von dem Satze 6. zu unterscheiden; denn für $m_1 = 2$ geht 6. in 5. über, weil dann $r_1 = -1$ wird, und nach Bd. I, §. 171

$$(r_1, \eta)^m = (-1, \eta)^m = \sqrt{p}^{\,m}$$

ist [1]).

Fassen wir das Ergebniss der Sätze 3. bis 6. in eine Formel zusammen, so ergiebt sich, wenn ε ein Einheitsfunctional, φ irgend ein Functional des Körpers Ω_m bedeutet, und p eine Reihe von Primzahlen durchläuft, die congruent mit 1 nach dem Modul q sind, worunter dieselbe Primzahl p auch mehrmals vorkommen kann,

$$(12) \qquad \omega = (r, x_0)^m = \varepsilon\, \varphi^m \prod^{p} (r^{m_2}, \eta)^m.$$

---

[1]) In des Verfassers Abhandlung in Bd. 8 der Acta mathematica ist es versäumt, den Fall des Satzes 5. besonders hervorzuheben.

Die in diesen Formeln vorkommenden Resolventen der Kreistheilung (r^{m_2}, η) sind Kreistheilungszahlen in einem höheren Körper. Ihre m^{ten} Potenzen sind aber im Körper Ω_m enthaltene Zahlen, die durch die Substitution (r, r^n) in

$$(r^{n\, m_2}, \eta)^m$$

übergehen. Ebenso sind die Verbindungen

$$(13) \qquad (r^{n\, m_2}, \eta)^{-1}\, (r^{m_2}, \eta)^n$$

im Körper Ω_m enthalten [§. 174, (9), (11)]. Diese Resolventen sind specielle Fälle der allgemeinen Resolvente (r, x_0). Aus (12) erhalten wir, wenn wir mit φ_n, ε_n die conjugirten Functionale zu φ und ε bezeichnen

$$(14) \qquad \omega_n = \varepsilon_n\, \varphi_n^m \prod^p (r^{m_2 n}, \eta)^m.$$

Diese Formel lehrt uns die wichtigsten Eigenschaften der Functionale φ_n und ε_n kennen, zunächst:

7. Die Functionale φ_n^m sind mit Zahlen des Körpers Ω_m associirt, gehören also der Hauptclasse an (§. 152).

Nach 1. ist $\omega_n^{-1}\, \omega_1^n = \alpha^m$ die m^{te} Potenz einer Zahl Ω_m. Da auch die Verbindungen (13) Zahlen in Ω_m sind, so können wir

$$\prod^p (r^{m_2 n}, \eta)^{-1}\, (r^{m_2}, \eta)^n = \frac{\alpha}{\beta}$$

setzen, und erhalten aus (14)

$$\varepsilon_n^{-1}\, \varepsilon_1^n\, (\varphi_n^{-1}\, \varphi_1^n)^m = \beta^m,$$

worin β eine Zahl in Ω_m ist.

Daraus geht hervor, dass das Product

$$\beta\, \varphi_n\, \varphi_1^{-n} = \varepsilon$$

ein Einheitsfunctional des Körpers Ω_m ist, und daraus ergeben sich für die Functionale φ_n und die Einheitsfunctionale ε_n die folgenden beiden Sätze:

8. Die conjugirten Functionale φ_n haben die Eigenschaft, dass alle Producte

$$\varphi_n\, \varphi_1^{-n}$$

der Hauptclasse angehören.

9. Die Einheitsfunctionale ε_n haben die Eigenschaft, dass die Producte

$$\varepsilon_n\, \varepsilon_1^{-n} = \varepsilon^m$$

m^{te} Potenzen von Einheitsfunctionalen sind.

Es kommt nun für den Beweis des Haupttheorems I. alles auf den Beweis der beiden Sätze an, die aus den Eigenschaften der Functionale φ und ε zu folgern sind:

A. Die Functionale φ_n gehören der Hauptclasse an.

Können wir dieses Lemma voraussetzen, so ist φ_n mit einer Zahl α_n associirt, und wir können die Formel (14) mit etwas veränderter Bedeutung von ε_n so darstellen:

$$\omega_n = \varepsilon_n \alpha_n^m \prod^{p} (r^{m_s n}, \eta)^m. \tag{15}$$

In dieser Formel ist aber ε_n eine numerische Einheit des Körpers Ω_m, die dem Satze 9. genügt.

Können wir also aus dem Satze 9. noch das zweite Lemma beweisen:

B. Eine numerische Einheit ε_n des Körpers Ω_m, die dem Satze 9. genügt, ist die m^{te} Potenz einer Einheit in Ω_m, multiplicirt mit einer Potenz von r;

so können wir in (15) die m^{te} Wurzel ziehen, und erhalten, wenn mit ϱ eine Einheitswurzel von möglicherweise höherem Grade als m und mit α eine Zahl des Körpers Ω_m bezeichnet wird:

$$(r, x_0) = \varrho\, \alpha \prod^{p} (r^{m_s}, \eta), \tag{16}$$

wo nun rechts lauter Kreistheilungszahlen stehen und wodurch daher das Theorem I. erwiesen ist.

§. 182.

Beweis des ersten Hülfssatzes für ein ungerades m.

Wir haben im vorigen Paragraphen den Beweis des Theorems I. von zwei Hülfssätzen abhängig gemacht, deren Beweis nun ferner zu suchen ist.

Wir formuliren den ersten dieser Hülfssätze so:

a) Ist φ_n ein System von Null verschiedener conjugirter Functionale des Körpers Ω_m, von denen bekannt ist, dass

$$\varphi_n^m \text{ und } \varphi_n^{-1} \varphi_1^n$$

der Hauptclasse angehören, so gehören die Functionale φ selbst der Hauptclasse an.

Der Satz wird bewiesen sein, wenn von irgend einer Potenz φ^k von φ, deren Exponent nicht durch q theilbar ist, bewiesen werden kann, dass sie der Hauptclasse angehört. Denn sind α, β Zahlen in Ω_m und ist

$$\varphi^m = \varepsilon' \alpha, \quad \varphi^k = \varepsilon'' \beta,$$

so können wir die ganzen rationalen Zahlen x, y so bestimmen, dass

$$m x + k y = 1$$

wird, und dann wird

$$\varphi = \varphi^{m x} \varphi^{k y} = \varepsilon''' \alpha^x \beta^y,$$

also ist auch, wenn $\varepsilon', \varepsilon'', \varepsilon'''$ Einheiten sind, φ selbst mit einer Zahl associirt.

Nach dem heutigen Stande der Sache ist der Beweis für ein gerades m auf einem ganz anderen Wege zu führen, als für ein ungerades, und wir beschäftigen uns also zunächst mit dem leichteren Falle des ungeraden m [1]).

Die in a) über φ_n gemachten Voraussetzungen können wir, wenn α, β wieder irgend welche Zahlen des Körpers Ω_m und ε Einheitsfunctionale bedeuten, durch die beiden Formeln ausdrücken:

(1) $$\varphi_n^m = \varepsilon \beta,$$

(2) $$\varphi_n = \varepsilon \alpha \varphi_1^n.$$

Wir werden nun die Aufgabe schrittweise lösen.

Ist zunächst, wie früher, σ der in q enthaltene Primfactor, der eine in Ω_m existirende Zahl ist, und σ^k die in φ enthaltene Potenz von σ, so setzen wir

(3) $$\varphi = \sigma^k \psi,$$

worin ψ ein zu q theilerfremdes Functional bedeutet, das denselben Bedingungen (1), (2) wie φ genügt, und wenn eines von beiden in die Hauptclasse gehört, so gilt das auch vom anderen. Der Satz a) braucht also nur noch unter der Voraussetzung bewiesen zu werden, dass φ theilerfremd zu q ist.

Es sei nun p eine von q verschiedene Primzahl, die in Primfactoren zerlegt den Ausdruck hat:

(4) $$p = \prod^{\xi} \mathfrak{p}_{\xi},$$

---

[1]) Vgl. übrigens den neuen Beweis von Hilbert, bei dem der Unterschied zwischen geradem und ungeradem m weit mehr zurücktritt (S. 648).

worin ξ die in §. 172 näher bestimmte Zahlenreihe durchläuft. Es möge $\mathfrak{p}_\xi^{k_\xi}$ die in φ enthaltene Potenz von $\mathfrak{p}_\xi$ sein, so dass, wenn wir

$$\varphi = \chi \prod^{\xi} \mathfrak{p}_\xi^{k_\xi}$$

setzen, χ theilerfremd zu p und mit keinen anderen Primzahlen verwandt ist (s. den Schluss von §. 173), als φ selbst. Daraus ergiebt sich

(5) $$\varphi_n = \chi_n \prod^{\xi} \mathfrak{p}_{n\xi}^{k_\xi},$$

und hierin lassen wir n abermals die Reihe der Zahlen ξ durchlaufen. Setzen wir noch

$$\psi = \prod^{\xi} \chi_\xi,$$

so ist auch ψ theilerfremd zu p und mit keinen anderen Primzahlen verwandt als φ, und wir erhalten aus (5) mit Benutzung von (4):

(6) $$\prod^{\xi} \varphi_\xi = \psi\, p^{\Sigma k_\xi},$$

und daraus ergiebt sich, dass das Functional ψ denselben beiden Bedingungen (1), (2) genügt, wie φ.

Es zeigt sich ferner, dass, wenn die φ_ξ in der Hauptclasse liegen, auch ψ in der Hauptclasse enthalten ist.

Wenn aber $p - 1$ nicht durch q theilbar ist, so können wir auch das Umgekehrte schliessen.

Denn nach (2) ist φ_ξ äquivalent mit φ^ξ und folglich ist:

$$\prod^{\xi} \varphi_\xi \text{ äquivalent } \varphi^{\Sigma \xi},$$
$$\text{äquivalent } \psi,$$

und wenn ψ mit einer Zahl associirt ist, so gilt dasselbe von $\varphi^{\Sigma\xi}$. Nach dem Satze §. 172 ist aber, wenn $p - 1$ nicht durch q theilbar ist, $\Sigma\, \xi$ auch nicht durch q theilbar, und folglich ist auch φ selbst in der Hauptclasse enthalten.

Diese Betrachtung können wir nun, wenn ψ noch mit weiteren Primzahlen, die nach dem Modul q nicht mit 1 congruent sind, verwandt ist, wiederholen, und kommen so zu dem Satze:

Der Satz a) ist allgemein bewiesen, wenn er unter der Voraussetzung bewiesen werden kann, dass φ nur mit solchen Primzahlen verwandt ist, die nach dem Modul q mit 1 congruent sind.

Machen wir diese Voraussetzung über die Functionale φ_n, so können wir das Kummer'sche Theorem in der Fassung des §. 174, 3. anwenden.

Wir bezeichnen in der Folge mit ε Einheitsfunctionale, auf deren genauere Kenntniss nichts ankommt, und setzen

$$(7) \qquad \Phi_n = \prod^t \varphi_{n t'}^t = \varepsilon \vartheta_n^m,$$

wenn t die durch q nicht theilbaren Reste von m, die kleiner als m sind, durchläuft, und t' durch $t t' \equiv 1 \pmod m$ bestimmt ist. Dann ist ϑ_n eine Kreistheilungszahl in einem höheren Körper, deren m^{te} Potenz in Ω_m enthalten ist und die der zweiten Bedingung genügt, dass

$$(8) \qquad \vartheta_n^{-1} \vartheta_1^n = \alpha$$

eine Zahl des Körpers Ω_m ist.

Wir führen nun ein vielfach gebrauchtes Zeichen ein, indem wir unter $E(x)$ die grösste ganze Zahl verstehen, die in der reellen Zahl x enthalten ist, und unter (x) den Rest, der stets ein echter Bruch ist, und, wenn x selbst eine ganze Zahl sein sollte, gleich Null zu setzen ist. Dann ist

$$(9) \qquad x = E(x) + (x).$$

Ist x eine ganze Zahl, so ist nach dieser Bezeichnungsweise

$$m\left(\frac{x}{m}\right)$$

auch eine ganze Zahl, und zwar der kleinste positive Rest der Theilung von x durch m.

In der Formel (7) ist der Index der Functionale φ nur nach dem Modul m bestimmt. Der Exponent aber ist auf seinen kleinsten Rest nach dem Modul m reducirt. Ersetzen wir also in (7) den Index t' durch $n' t'$, so muss t durch den Rest der Division von $n t$ durch m, d. h. [nach (9)] durch

$$m\left(\frac{n t}{m}\right) = n t - m E\left(\frac{n t}{m}\right)$$

ersetzt werden, und wir können setzen

$$\Phi_n = \prod^t \varphi_{t'}^{n t - m E\left(\frac{n t}{m}\right)} = \varepsilon \vartheta_n^m,$$

andererseits ist

$$\Phi_1 = \prod^t \varphi_{t'}^t = \varepsilon \vartheta_1^m,$$

also nach (8)

$$(10) \qquad \Phi_1^n \, \Phi_n^{-1} = \prod^t \varphi_{t'}^{m\,E\left(\frac{n\,t}{m}\right)} = \varepsilon\, \alpha^m.$$

Hiernach ist der Quotient

$$\left(\frac{\prod\limits^t \varphi_{t'}^{E\left(\frac{n\,t}{m}\right)}}{\alpha}\right)^m$$

ein Einheitsfunctional, und da er zugleich die m^{te} Potenz eines Functionals in Ω_m ist, so ist die Basis dieser Potenz auch eine Einheit, d. h. es ist

$$\prod^t \varphi_{t'}^{E\left(\frac{n\,t}{m}\right)} = \varepsilon\, \alpha,$$

und es gehört dies Product der Hauptclasse an. Nun ist aber nach unserer Voraussetzung

$$\varphi_{t'} \text{ äquivalent mit } \varphi^{t'},$$

und daher ist

$$\prod^t \varphi_{t'}^{E\left(\frac{n\,t}{m}\right)} \text{ äquivalent mit } \varphi^{\sum\limits^t t'\,E\left(\frac{n\,t}{m}\right)},$$

und dies gilt für jedes beliebige durch q nicht theilbare n.

Können wir also nachweisen, dass sich n so bestimmen lässt, dass auch die Summe

$$S_n = \sum^t t'\,E\left(\frac{n\,t}{m}\right)$$

durch q nicht theilbar ist, so haben wir das Theorem a) bewiesen.

Wir wollen zunächst eine Umformung der Summe S_n vornehmen, durch die die Frage auf den weit einfacheren Fall zurückgeführt wird, in dem m eine Primzahl ist.

Wir setzen, wenn m eine höhere als die erste Potenz von q ist,

$$m = q\,m', \quad t = t_1 + q\,t_2, \quad \begin{array}{l} t_1 = 1, 2, \ldots, q - 1 \\ t_2 = 0, 1, \ldots, m' - 1. \end{array}$$

Darin ist m' noch eine Potenz von q, der Summationsbuchstabe t_1 durchläuft die Zahlenreihe $1, 2, \ldots, q - 1$, und t_2 die Zahlenreihe $0, 1, 2, \ldots, m' - 1$. Wir bestimmen t_1' aus der Congruenz

$$t_1\, t_1' \equiv 1 \pmod q$$

und erhalten

$$t' \equiv t_1' \pmod q.$$

Es ist dann

$$(11)\qquad S_n = \sum^{t} t' E\left(\frac{tn}{m}\right) \equiv \sum^{t_1} t_1' \sum^{t_2} E\left(\frac{n t_2}{m'} + \frac{n t_1}{m}\right) \pmod q.$$

Wir nehmen jetzt $n < q$ an, also auch $n t_1 < m$, so dass $n t_1 : m$ ein echter Bruch ist. Dann ist

$$\text{a)}\qquad E\left(\frac{n t_2}{m'} + \frac{n t_1}{m}\right) \text{ entweder } = E\left(\frac{n t_2}{m'}\right)$$

$$\text{b)}\qquad \text{oder } = E\left(\frac{n t_2}{m'}\right) + 1,$$

und zwar tritt der Fall b) nur dann ein, wenn zwischen

$$\frac{n t_2}{m'} \text{ und } \frac{n t_2}{m'} + \frac{n t_1}{m}$$

eine ganze Zahl liegt. Dies ist aber nur dann der Fall, wenn der Unterschied zwischen $n t_2 : m'$ und der nächst grösseren ganzen Zahl kleiner als $n t_1 : m$ ist, also wenn

$$(12)\qquad E\left(\frac{n t_2}{m'}\right) + 1 - \frac{n t_2}{m'} < \frac{n t_1}{m}.$$

Lassen wir in dem Ausdrucke auf der linken Seite von (12)

$$(13)\qquad E\left(\frac{n t_2}{m'}\right) + 1 - \frac{n t_2}{m'}$$

t_2 alle seine Werthe durchlaufen, so erhalten wir lauter positive, die Einheit nicht übersteigende rationale Brüche mit dem Nenner m', von denen keine zwei einander gleich sind. Denn wären zwei der Werthe, die aus (13) durch Substitution von t_2', t_2'' für t_2 entstehen, einander gleich, so müsste $\frac{n(t_2' - t_2'')}{m'}$ eine ganze Zahl sein, was, da n relativ prim zu m' und $t_2' - t_2''$ kleiner als m' ist, nicht sein kann. Die Ausdrücke (13) durchlaufen daher in irgend einer Reihenfolge die Zahlenwerthe

$$(14)\qquad \frac{1}{m'}, \frac{2}{m'}, \ldots, \frac{m'-1}{m'}, 1,$$

und wenn a einen beliebigen positiven Bruch bedeutet, so ist $E(m'a)$ die Anzahl der Zahlen der Reihe (14), die nicht grösser als a sind. Nach (12) ist daher die Anzahl der Werthe von t_2, für die der Fall b) eintritt, gleich $E\left(\frac{n t_1}{q}\right)$, und es ergiebt sich

$$\sum^{t_2} E\left(\frac{n t_2}{m'} + \frac{n t_1}{m}\right) = \sum^{t_2} E\left(\frac{n t_2}{m}\right) + E\left(\frac{n t_1}{q}\right).$$

Um S_n zu bilden, multipliciren wir diese Gleichung mit t_1' und summiren. Dadurch ergiebt sich

$$S_n \equiv \sum^{t_1'} t_1' \sum^{t_2} E\left(\frac{n\,t_2}{m}\right) + \sum^{t_1} t_1' \,E\left(\frac{n\,t_1}{q}\right) \pmod q.$$

Darin ist nun $\sum t_1' = \sum t_1 \equiv 0 \pmod q$, weil die t_1 paarweise die Summe q ergeben, und es folgt:

$$S_n \equiv \sum^{t_1} t_1' \,E\left(\frac{n\,t_1}{q}\right) \pmod q. \tag{15}$$

Die Summe, die hier auf der rechten Seite steht, ist ebenso gebildet, wie S_n selbst in dem Falle, wo m eine Primzahl ist. Für diesen Fall ergiebt sich aber

$$\frac{n\,t_1}{q} = E\left(\frac{n\,t_1}{q}\right) + \left(\frac{n\,t_1}{q}\right)$$

$$\frac{(q-n)\,t_1}{q} = E\left(\frac{(q-n)\,t_1}{q}\right) + \left(\frac{(q-n)\,t_1}{q}\right),$$

und daraus durch Addition

$$t_1 = E\left(\frac{n\,t_1}{q}\right) + E\left(\frac{(q-n)\,t_1}{q}\right) + \left(\frac{n\,t_1}{q}\right) + \left(\frac{(q-n)\,t_1}{q}\right),$$

und dabei kann die Summe der beiden positiven echten Brüche, die doch eine ganze Zahl sein muss, nur den Werth 1 haben. Es folgt also

$$E\left(\frac{n\,t_1}{q}\right) + E\left(\frac{(q-n)\,t_1}{q}\right) = t_1 - 1,$$

und daraus durch Multiplication mit t_1' und Summation über alle Werthe von t_1 von 1 bis $q-1$

$$\sum^{t_1} t_1' \,E\left(\frac{n\,t_1}{q}\right) + \sum^{t_1} t_1' \,E\left(\frac{(q-n)\,t_1}{q}\right) \equiv -1 \pmod q.$$

Folglich können sicher nicht beide Summen auf der linken Seite durch q theilbar sein. Dann zeigt der Ausdruck (15), dass von den beiden Summen S_n und S_{q-n} gewiss eine durch q untheilbar ist.

Dies aber war zu beweisen.

§. 183.

Beweis des zweiten Hülfssatzes für ein ungerades m.

Das zweite Lemma, was nach §. 181 noch zu beweisen ist, ist folgendes:

2. Ist ε_n ein System conjugirter numerischer Einheiten des Körpers Ω_m, das der Bedingung genügt, dass

(1) $$\varepsilon_n \varepsilon_1^{-n} = \mathfrak{E}^m$$

die m^{te} Potenz einer Einheit in Ω_m ist, so sind die ε_n selbst m^{te} Potenzen von Einheiten in Ω_m, multiplicirt mit einer Einheitswurzel der Form r^{nk}.

Auch dieser Beweis ist für den Fall eines ungeraden m ganz elementar. Wir betrachten daher hier zunächst diesen Fall.

Nach §. 178, 1. können wir jede Einheit des Körpers Ω_m in der Form darstellen:

(2) $$\varepsilon = \pm\, r^k \mathfrak{E}(r), \quad \varepsilon_n = \pm\, r^{nk} \mathfrak{E}(r^n),$$

worin $\mathfrak{E}(r)$ eine reelle Einheit des Körpers Ω_m ist. Es genügt also $\mathfrak{E}(r)$ der Bedingung

(3) $$\mathfrak{E}(r) = \mathfrak{E}(r^{-1}),$$

woraus sich nach (2) ergiebt:

(4) $$\varepsilon_1 \varepsilon_{-1} = \mathfrak{E}(r)^2;$$

aus (1) aber findet sich, wenn man $n = -1$ setzt,

$$\varepsilon_1 \varepsilon_{-1} = \mathfrak{E}^m,$$

d. h. die linke Seite von (4) ist die m^{te} Potenz einer Einheit in Ω_m, und es ist also auch

(5) $$\mathfrak{E}(r)^2 = \mathfrak{E}^m$$

die m^{te} Potenz einer solchen Einheit.

Da nun m ungerade ist, so lässt sich die ganze rationale Zahl x so bestimmen, dass

(6) $$2x + m = 1$$

wird, und daraus folgt

$$\mathfrak{E}(r) = \mathfrak{E}(r)^{2x} \mathfrak{E}(r)^m.$$

Wenn wir also nach (5)

$$\mathfrak{G}^x \mathfrak{G}(r) = e(r)$$

setzen, so folgt

(7) $$\mathfrak{G}(r) = e(r)^m.$$

Durch (7) ist aber der Satz 2. bewiesen und damit zugleich für ein ungerades m das ganze Theorem I.

Auch dieser Schluss versagt für ein gerades m, weil dann die Gleichung (6) nicht mehr lösbar ist.

§. 184.

Vorläufiges über den Fall eines geraden m.

Für den Fall, dass m eine Potenz von 2 ist, schlagen wir einen ganz anderen Weg ein, über den hier zunächst einige vorläufige Bemerkungen Platz finden mögen.

Wir haben schon im §. 182 gesehen, dass das erste Lemma bewiesen ist, wenn wir nachweisen können, dass irgend eine Potenz von φ, deren Exponent nicht durch q theilbar ist, zur Hauptclasse gehört. Dabei ist von den beiden Eigenschaften des Functionals φ nur die erste benutzt, dass die m^{te} Potenz von φ in der Hauptclasse enthalten ist.

Nun kennen wir nach den allgemeinen Sätzen in §. 154 in jedem Körper einen Exponenten h, nämlich die Anzahl der Idealclassen, für den φ^h zur Hauptclasse gehört, wenn φ ein beliebiges Functional in diesem Körper ist.

Wenn wir also beweisen können, dass die Classenzahl h im Körper Ω_m, wenn m eine Potenz von 2 ist, eine ungerade Zahl ist, so ist damit ohne alles Weitere das Lemma 1. bewiesen.

Dies soll das Ziel unserer Betrachtungen in den nächsten Abschnitten sein.

In Bezug auf das zweite Lemma liegt die Sache ähnlich. Hier kann man aus den Voraussetzungen in §. 183, 2. ganz wie oben die Formel §. 183, (5) herleiten, aus der aber nur zu schliessen ist, dass $\mathfrak{G}(r)$ die $\frac{1}{2}m^{te}$ Potenz einer reellen Einheit $e(r)$ ist.

Nehmen wir also das erste Lemma als bewiesen an, so ergiebt die Formel §. 181, (14):

(1) $$(r^n, x_0) = \varrho_n \sqrt{e(r^n)}\, \alpha_n \Pi (r^{m_1 n}, \eta),$$

worin ρ_n eine Einheitswurzel vom Grade m^2, und α_n eine Zahl in Ω_m ist, und es wäre noch zu beweisen, dass $e(r^n)$ das Quadrat einer Einheit in Ω_m ist.

Da $e(r)$ eine reelle Einheit ist, so ist

(2) $$e(r^n) = e(r^{-n}),$$

und wir wollen noch festsetzen, dass das Vorzeichen der Wurzel so bestimmt sei (was wir bei passender Annahme über ρ_n immer annehmen können), dass

(3) $$\sqrt{e(r^n)} = \sqrt{e(r^{-n})}.$$

Das Product $(r^n, x_0)\,(r^{-n}, x_0)$ ist nach der Voraussetzung eine Zahl des Körpers Ω_m, die sich durch die Substitution (r, r^{-1}) nicht ändert, d. h. eine reelle Zahl. Ferner ist nach §. 174, (5)

$$(r^{m_2 n}, \eta)\,(r^{-m_2 n}, \eta) = \pm p,$$

also gleichfalls reell. Ebenso ist $\alpha_n \alpha_{-n}$ reell, und daraus ergiebt sich nach (1), dass

$$\rho_n \rho_{-n} = \frac{(r^n, x_0)\,(r^{-n}, x_0)}{e(r^n)\,\alpha_n \alpha_{-n}\,\Pi\,(r^{m_2 n}, \eta)\,(r^{-m_2 n}, \eta)}$$

eine reelle Zahl ist, die, weil sie eine Einheitswurzel ist, nur $= \pm 1$ sein kann.

Nun können wir in der hieraus für $n = 1$ sich ergebenden Gleichung

$$(r, x_0)\,(r^{-1}, x_0) = \pm\, e(r)\,\alpha_1 \alpha_{-1}\,\Pi\,(\pm p)$$

jede Substitution (r, r^n) ausführen, woraus hervorgeht, dass das Zeichen von $\rho_n \rho_{-n}$ von n unabhängig ist, dass also

(4) $$\rho_n \rho_{-n} = \rho_1 \rho_{-1} = \pm 1$$

ist. Nun leiten wir aus (1) weiter her:

(5) $$\rho_n \rho_1^{-1} \sqrt{e(r^n)}\,\sqrt{e(r)}^{-n} = \frac{(r^n, x_0)\,(r, x_0)^{-n}}{\alpha_n \alpha_1^{-1}\,\Pi\,(r^{m_2 n}, \eta)\,(r^{m_2}, \eta)^{-n}},$$

und die rechte Seite ist eine Zahl des Körpers Ω_m. Die linke Seite zeigt aber, dass es eine Einheit ist, und wir können demnach, wenn $\mathfrak{E}(r)$ eine reelle Einheit bedeutet,

(6) $$\rho_n \rho_1^{-1} \sqrt{e(r^n)}\,\sqrt{e(r)}^{-n} = r^k\,\mathfrak{E}(r)$$

setzen. Substituiren wir diesen Werth in die Formel (5) und machen die Substitution (r, r^{-1}), so ergiebt sich

(7) $$\rho_{-n} \rho_{-1}^{-1} \sqrt{e(r^n)}\,\sqrt{e(r)}^{-n} = r^{-k}\,\mathfrak{E}(r),$$

und durch Multiplication von (6) und (7) mit Rücksicht auf (4)

(8) $$e(r^n)\, e(r)^{-n} = \mathfrak{E}(r)^2.$$

In unseren Betrachtungen über die Classenzahl wird sich noch der Satz ergeben:

> Eine Einheit $e(r)$ des reellen Körpers H_m, die mit allen ihren Conjugirten positiv ist, ist das Quadrat einer Einheit im Körper H_m.

Die Formel (8) zeigt aber, dass der Einheit $\pm e(r)$ diese Eigenschaft zukommt, und dass daher $e(r)$ (da auch $-1 = i^2$ das Quadrat einer Einheit ist) das Quadrat einer Einheit des Körpers Ω_m ist.

Damit ist die Frage auf den Beweis der beiden erwähnten Sätze zurückgeführt, der sich als Schlussstein einer langen, aber an interessanten Beziehungen äusserst reichen Kette von Betrachtungen ergiebt, denen die nächsten Abschnitte gewidmet sein sollen.

Dreiundzwanzigster Abschnitt.

Classenzahl.

---

§. 185.

Der Dirichlet'sche Satz über die Einheiten.

Die Untersuchungen über die Anzahl der Idealclassen in einem algebraischen Körper, die uns nun die nothwendigen Ergänzungen der Beweise des vorigen Abschnittes geben sollen, bedienen sich der Methoden, die Dirichlet in die Zahlentheorie eingeführt hat [1]).

Sie sind nicht mehr rein algebraisch, insofern dabei auch transcendente Functionen und Zahlen, wie der natürliche Logarithmus und die Zahl π vorkommen. Auch wird von Grenzübergängen, wie in der Integralrechnung, Gebrauch gemacht, aus denen wir schon in §. 156 ein schönes Resultat gezogen haben.

Die Untersuchungen, von denen wir zunächst zu handeln haben, sind ganz allgemein, d. h. sie gelten für jeden algebraischen Zahlkörper, und es bietet keinen Vortheil der Einfachheit, sie auf specielle Körper, wie etwa die Kreistheilungskörper, zu beschränken.

---

[1]) Dirichlet, Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. Crelle's Journal, Bd. 19, 21. Dirichlet's Werke, Bd. I (1839, 1840). (Hierher gehören übrigens auch die nachgelassenen Abhandlungen von Gauss, „De nexu inter multitudinem classium etc." Gauss' Werke, Bd. II.) Die Anwendung dieser Principien auf die Kreistheilungszahlen hat zuerst Kummer gemacht [Crelle's Journal, Bd. 35, 40 (1847, 1850); Liouville's Journal, Bd. 16 (1851)]. Die allgemeine Theorie der Einheiten ist gleichfalls von Dirichlet begründet [Dirichlet's Werke, Bd. I, S. 622, 633, 639 (1840, 1842, 1846)]. Die allgemeine Theorie der Einheiten und die Bestimmung der Classenzahlen hat Dedekind gegeben: Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Auflage, §. 183 f. Minkowski, Geometrie der Zahlen.

Es sei also Ω ein Körper n^{ten} Grades, und

(1) $$\Omega_1, \Omega_2, \ldots, \Omega_n$$

die conjugirten Körper. Die irreducible Gleichung n^{ten} Grades, deren Wurzeln uns diese conjugirten Körper bestimmen, wird im Allgemeinen sowohl reelle als imaginäre Wurzeln haben, von denen aber die letzteren immer paarweise vorkommen, so dass zu jedem imaginären Körper $\Omega^{(i)}$ ein anderer gehört, dessen Zahlen mit denen von $\Omega^{(i)}$ conjugirt imaginär sind, der also aus $\Omega^{(i)}$ durch die Substitution $(i, -i)$ hervorgeht.

Solche imaginäre Paare fassen wir zu einer Einheit zusammen und bezeichnen die Anzahl der reellen Körper und der Paare imaginärer Körper der Reihe (1) mit ν. Sind alle conjugirten Körper reell, so ist $n = \nu$; sind sie alle imaginär, so ist $n = 2\nu$.

Ausser im Falle des rationalen Körpers ist ν nur noch in dem Falle eines imaginären quadratischen Körpers $= 1$. Sonst ist ν immer grösser als 1.

Die Anzahl der imaginären Paare ist $n - \nu$, und die Anzahl der reellen Körper $2\nu - n$.

In der Determinante, durch die in §. 145 die Quadratwurzel aus der Grundzahl, $\sqrt{\Delta}$, definirt ist, vertauschen sich durch die Substitution $(i, -i)$ je zwei conjugirt imaginäre Reihen, und $\sqrt{\Delta}$ wechselt also sein Zeichen dann, wenn diese Zahl ungerade ist, sonst nicht. Im ersten Falle ist $\sqrt{\Delta}$ imaginär, im zweiten reell. Daraus ergiebt sich also, dass die Grundzahl Δ des Körpers Ω positiv oder negativ ist, je nachdem $n - \nu$ gerade oder ungerade ist.

Behalten wir von zwei conjugirt imaginären Körpern nur den einen bei, so ergiebt sich die Reihe der conjugirten Körper

$$\Omega_1, \Omega_2, \ldots, \Omega_\nu,$$

denen wir ein Zeichensystem

$$\delta_1, \delta_2, \ldots, \delta_\nu$$

mit der Bestimmung zuordnen, dass $\delta_s = 1$ sein soll, wenn Ω_s reell, und $= 2$, wenn Ω_s imaginär ist, also $\Sigma\, \delta_s = n$.

Es möge η eine von Null verschiedene Zahl des Körpers Ω bedeuten und

$$\eta_1, \eta_2, \ldots, \eta_n$$

die conjugirten Zahlen. Diesem Zahlensysteme ordnen wir ein anderes Zahlensystem zu

$$\lambda_1, \lambda_2, \ldots, \lambda_n,$$

das wir durch die Gleichung

(2) $$\lambda_s = \delta_s \log |\eta_s|$$

definiren, worin $|\eta_s|$ den absoluten Werth von η_s und $\log |\eta_s|$ den reellen natürlichen Logarithmus der positiven Zahl $|\eta_s|$ bedeutet. Ist Ω_s reell und das Zeichen $\pm$ so gewählt, dass $\pm\, \eta_s$ positiv ist, so ist

$$\lambda_s = \log (\pm\, \eta_s).$$

Ist aber η_s, η_s' ein imaginäres Paar, so ist

$$\lambda_s = \log \eta_s \eta_s',$$

und zu η_s und η_s' gehört dasselbe λ_s, so dass die Anzahl der verschiedenen λ_s gleich ν ist. Aus dieser Bestimmung ergiebt sich noch

(3) $$\lambda_1 + \lambda_2 + \cdots + \lambda_\nu = \log N_a(\eta),$$

wenn, wie früher, N_a die absolute Norm bedeutet.

Die Zahlen $\lambda_1, \lambda_2, \ldots, \lambda_\nu$ wollen wir die **conjugirten Logarithmen** der Zahl η nennen.

Wenn η eine **ganze** Zahl des Körpers Ω ist, so ist die absolute Norm eine **natürliche** Zahl, die nur dann $= 1$ ist, wenn η eine Einheit ist, und daraus folgt nach (3):

1. Die Summe der conjugirten Logarithmen einer ganzen Zahl η ist positiv, und nur dann gleich Null, wenn η eine Einheit ist.

Bedeutet $\omega_1, \omega_2, \ldots, \omega_n$ eine Basis der ganzen Zahlen in Ω (eine Minimalbasis von Ω, §. 145), und $\omega_{1,s}, \omega_{2,s}, \ldots, \omega_{n,s}$ für $s = 1, 2, \ldots, n$ die conjugirten Zahlen, so lassen sich alle ganzen Zahlen des Körpers Ω_s in der Form darstellen:

(4) $$\eta_s = x_1\, \omega_{1,s} + x_2\, \omega_{2,s} + \cdots + x_n\, \omega_{n,s},$$

mit ganzen rationalen Coëfficienten $x_1, x_2, \ldots, x_n$. Die Determinante dieses Systemes

$$\Sigma \pm \omega_{1,1}\, \omega_{2,2} \ldots \omega_{n,n} = \sqrt{\Delta}$$

ist die Quadratwurzel aus der Discriminante Δ des Körpers, und demnach immer von Null verschieden. Demnach lässt sich das System (4) nach den Unbekannten $x_1, x_2, \ldots, x_n$ auflösen, und wenn wir nun festsetzen, dass die absoluten Werthe der Zahlen η_s nicht über eine gewisse Grenze hinausgehen sollen, so ergeben sich aus diesen Auflösungen Grenzen für die ganzen rationalen Zahlen x_i.

Diese einfache Bemerkung liefert uns den folgenden wichtigen Satz:

2. Es giebt in einem algebraischen Körper Ω nur eine endliche Anzahl ganzer Zahlen η von der Beschaffenheit, dass die absoluten Werthe der conjugirten Zahlen η_s unter einer gegebenen Grenze liegen.

Wir machen jetzt von dem allgemeinen Satze §. 155, (25) Gebrauch, nach dem, wenn $f(x_1, x_2, \ldots, x_n)$ irgend eine positive quadratische Form von n Variablen mit der Determinante D ist, die Variablen x_i sich als ganze rationale Zahlen, nicht alle verschwindend, so bestimmen lassen, dass

$$f(x_1, x_2, \ldots, x_n) < n \sqrt[n]{0{,}404\, D},$$

d. h. kleiner als eine von der Determinante D allein abhängige Zahl wird.

Diesen Satz wenden wir, wie im §. 156, auf die Form an:

$$f(x_1, x_2, \ldots, x_n) = \frac{|\eta_1|^2}{c_1^2} + \frac{|\eta_2|^2}{c_2^2} + \cdots + \frac{|\eta_n|^2}{c_n^2},$$

worin die η_s die Linearformen (4) sind, und im Falle eines reellen η_s

$$|\eta_s|^2 = (\eta_s)^2,$$

im Falle eines imaginären Paares η_s, η_s'

$$|\eta_s|^2 = |\eta_s'|^2 = \eta_s \eta_s'.$$

Im letzteren Falle ist $\eta_s \eta_s'$ die Summe zweier reeller Quadrate, und demnach ist, wenn die c_s reell angenommen werden, f eine positive Form. Wir wollen über die bis jetzt willkürlichen reellen Grössen c_s noch festsetzen, dass, wenn η_s, η_s' ein conjugirt imaginäres Paar bilden,

$$(5) \qquad c_s = c_s'$$

sein soll; ausserdem wollen wir die c_s noch der Bedingung unterwerfen:

$$(6) \qquad c_1 c_2 \ldots c_n = 1.$$

Die Determinante der Function f bilden wir, wie im §. 156, dadurch, dass wir sie zunächst als Form der Variablen $\eta_1, \eta_2, \ldots, \eta_n$ auffassen, und die Determinante dieser Form ist wegen (6) gleich ± 1. Die Determinante von f in Bezug auf die Variablen x_i ist also (Bd. I, §. 56), vom Vorzeichen abgesehen, gleich dem

Quadrate der Determinante der Linearformen η_s, d. h. der Grundzahl des Körpers Ω.

Daraus folgt, dass man eine von den c_s unabhängige, nur durch den Körper Ω bestimmte Zahl A finden kann, von der Art, dass, was auch die c_s sein mögen, $f(x_1, x_2, \ldots, x_n)$ für ganzzahlige nicht verschwindende x unter A heruntersinkt. Da f die Summe von positiven Summanden ist, so gilt dasselbe von jedem dieser Summanden, und damit ist der folgende Satz bewiesen:

3. Ist c_s ein beliebiges, den Bedingungen (5), (6) genügendes System reeller positiver Zahlen, so giebt es eine durch den Körper Ω allein bestimmte reelle Zahl A von der Art, dass man immer eine ganze Zahl η des Körpers Ω bestimmen kann, die mit ihren conjugirten Zahlen η_s den Bedingungen genügt

$$|\eta_s| < c_s A. \tag{7}$$

Beiläufig folgt hieraus, dass man in jedem algebraischen Körper Ω, ausgenommen dem rationalen und dem imaginären quadratischen, von Null verschiedene ganze Zahlen finden kann, deren absoluter Werth unter jede gegebene Grenze heruntersinkt.

Wir wollen den Ausdruck des Satzes 3. durch Einführung der conjugirten Logarithmen von η etwas umformen. Wir setzen $\log A = k$, so dass k eine durch Ω bestimmte reelle Zahl ist, ferner

$$c_s = e^{\frac{\gamma_s u}{\delta_s}}, \tag{8}$$

worin u eine beliebige reelle Grösse sein kann, und die Zahlen γ_s wegen (5) und (6) der Bedingung genügen:

$$\gamma_1 + \gamma_2 + \cdots + \gamma_\nu = \sum_{1,\nu}^{i} \gamma_i = 0. \tag{9}$$

Da überdies

$$|\eta_s| = e^{\frac{\lambda_s}{\delta_s}}$$

ist, so folgt aus (7) und (8):

$$\lambda_s - \gamma_s u < k\,\delta_s. \tag{10}$$

Die Summe der ν Ausdrücke auf der linken Seite dieser Ungleichung ist wegen (9) gleich $\Sigma\,\lambda_s$, also nach dem Satze 1. nicht negativ, und wir finden

$$0 \gtreqless \sum^{s} (\lambda_s - \gamma_s u) < k\,n.$$

Daraus ergiebt sich wegen (10), dass ein Glied dieser Summe, $\lambda_s - \gamma_s u$, nicht kleiner sein kann, als $-(n - \delta_s)\, k$, weil sonst die Gesammtsumme negativ wäre, und wenn wir der Einfachheit halber die untere Grenze noch etwas kleiner nehmen

(11) $$-\, n k \delta_s < \lambda_s - \gamma_s u < k \delta_s.$$

Damit ist bewiesen, dass es für jedes gegebene System der Zahlen u, γ_s, wenn nur die Bedingung (9) erfüllt ist, eine ganze Zahl η des Körpers Ω giebt, die mit ihren conjugirten Zahlen den Grenzbedingungen (11) genügt.

Es sei nun ferner g_s ein System reeller Grössen, von dem wir nur verlangen, dass

$$\gamma_1 g_1 + \gamma_2 g_2 + \cdots + \gamma_\nu g_\nu = \alpha$$

von Null verschieden sei. Damit ist [nach (9)] ausgeschlossen, dass alle g_s einander gleich sind; wenn sie aber das nicht sind, so werden sich zu jedem gegebenen Systeme der g_s unendlich viele Systeme γ_s bestimmen lassen, die der Forderung (9) genügen.

Wird nun $k \sum \delta_s g_s = g$ gesetzt, so ergiebt sich aus (11) durch Multiplication mit g_s und Summation

(12) $$-\, n g + \alpha u < \sum g_s \lambda_s < g + \alpha u.$$

Nach dieser Grenzbedingung bestimmen wir nun, bei festgehaltenen g_s und α, eine Reihe von ganzen Zahlen

(13) $$\eta,\ \eta',\ \eta'',\ \eta''',\ \ldots,$$

indem wir für u eine Reihe von Annahmen machen:

$$u,\ u',\ u'',\ u''',\ \ldots,$$

die folgendermaassen näher bestimmt sind:

Wir wählen u zunächst so, dass

$$-\, n g + \alpha u = a, \quad g + \alpha u = a'$$

positiv werden; dann setzen wir

$$\delta = \frac{a' - a}{\alpha} = \frac{(n + 1)\, g}{\alpha},$$

und setzen

$$u' = u + \delta, \quad u'' = u' + \delta, \quad u''' = u'' + \delta, \quad \ldots,$$
$$a + \alpha\delta = a', \quad a' + \alpha\delta = a'', \quad a'' + \alpha\delta = a''', \ldots,$$

und erhalten so aus (12), wenn λ_s', λ_s'', ... die conjugirten Logarithmen von η', η'', ... sind:

$$(14)\qquad \begin{aligned} a &< \Sigma\, g_s \lambda_s < a' \\ a' &< \Sigma\, g_s \lambda_s' < a'' \\ a'' &< \Sigma\, g_s \lambda_s'' < a''' \\ &\ldots\ldots\ldots, \end{aligned}$$

und die Reihe dieser Ungleichungen lässt sich unbegrenzt fortsetzen.

Alle diese Zahlen η, η' η'', ... haben überdies nach (6) und (7) die Eigenschaft, dass ihre absoluten Normen N, N', N'', ... unter einer bestimmten endlichen Grenze e^{nk} bleiben.

Die Anzahl der möglichen Werthe von N, N', N'', ... ist also endlich, nämlich gewiss nicht grösser, als die grösste in e^{nk} enthaltene ganze Zahl. Ebenso ist die Anzahl aller möglichen Reste der Zahlen $x_1, x_2, \ldots, x_n$ [in (4)] nach allen Moduln N, N', N'', ... nur eine endliche, und daraus folgt, dass, wenn wir die Reihe der Zahlen (13) nur weit genug fortsetzen, in der Reihe zwei verschiedene Zahlen $\eta^{(h)}$, $\eta^{(k)}$ auftreten müssen, in denen $N^{(h)} = N^{(k)}$ und die Reste von $x_1, x_2, \ldots, x_n$ nach dem Modul $N^{(h)}$ genau dieselben sind.

Aus (14) aber folgt, wenn $h > k$ vorausgesetzt wird:

$$(15)\qquad \Sigma\, g_s (\lambda_s^{(h)} - \lambda_s^{(k)}) > 0.$$

Ist N die absolute Norm dieser beiden Zahlen $\eta^{(h)}$, $\eta^{(k)}$, so ist wegen der Uebereinstimmung der Reste der x die Differenz $\eta^{(h)} - \eta^{(k)}$ durch N theilbar. Andererseits ist nach §. 138 (13) die Zahl N durch $\eta^{(h)}$ theilbar, und folglich ist auch $\eta^{(h)} - \eta^{(k)}$ durch $\eta^{(h)}$ theilbar. Daraus ergiebt sich, dass auch $\eta^{(k)}$ durch $\eta^{(h)}$ und ebenso $\eta^{(h)}$ durch $\eta^{(k)}$ theilbar ist. Beide Zahlen sind also associirt, und wenn wir

$$\frac{\eta^{(h)}}{\eta^{(k)}} = \varepsilon$$

setzen, so ist ε eine Einheit des Körpers Ω.

Setzen wir ausserdem, indem wir mit $|\varepsilon_s|$ den absoluten Werth von ε_s bezeichnen,

$$(16)\qquad \delta_s \log |\varepsilon_s| = l_s,$$

so ergiebt sich aus (15):

$$(17)\qquad g_1 l_1 + g_2 l_2 + \cdots + g_\nu l_\nu > 0.$$

Dies beweist nun der Satz:

4. Ist $g_1, g_2, \ldots, g_\nu$ ein beliebiges System reeller Zahlen, die nicht alle einander gleich sind, so lässt sich in jedem algebraischen Körper Ω eine Einheit ε so bestimmen, dass die Summe
$$g_1 l_1 + g_2 l_2 + \cdots + g_\nu l_\nu$$
von Null verschieden ist, wenn l_s das System der conjugirten Logarithmen von ε ist.

Dieser wichtige Satz, der das Fundament für das Folgende ist, rührt, wenn auch in etwas veränderter Fassung, von Dirichlet her. Diese Formulirung ist von Minkowski gegeben.

§. 186.

Systeme unabhängiger Einheiten und Exponentensysteme der Einheiten.

Wenn wir in dem zuletzt bewiesenen Satze $g_1 = 1$, $g_2 = 0, \ldots, g_\nu = 0$ setzen, was, wenn wir von jetzt an $\nu > 1$ voraussetzen, gestattet ist, so folgt, dass es in Ω eine Einheit ε giebt, für die einer der conjugirten Logarithmen, l_1, von Null verschieden ist. Da jede Potenz von ε dieselbe Eigenschaft hat, so giebt es auch unendlich viele solche Einheiten.

Dieser Satz gestattet nun eine sehr wichtige Verallgemeinerung:

5. Ist $s \gtreqless \nu - 1$, so lässt sich im Körper Ω ein System von Einheiten mit den zugehörigen conjugirten Logarithmen
$$\begin{array}{l} \varepsilon_1 : l_{1,1}, l_{1,2}, \ldots, l_{1,\nu} \\ \varepsilon_2 : l_{2,1}, l_{2,2}, \ldots, l_{2,\nu} \\ \ldots\ldots\ldots\ldots\ldots \\ \varepsilon_s : l_{s,1}, l_{s,2}, \ldots, l_{s,\nu} \end{array} \tag{1}$$
derart bestimmen, dass eine beliebige der s-reihigen Determinanten der Matrix der $l_{h,k}$, etwa
$$L_s = \Sigma \pm l_{1,1}\, l_{2,2} \ldots l_{s,s}$$
von Null verschieden ist.

Für $s = 1$ ist der ausgesprochene Satz nach der am Eingange gemachten Bemerkung richtig. Wir nehmen also an, er

sei bewiesen für $s-1$ und leiten ihn durch vollständige Induction allgemein her. Dazu ordnen wir die Determinante L_s nach den Elementen der letzten Zeile, und schreiben sie so:

(2)
$$L_s = g_1 l_{s,1} + g_2 l_{s,2} + \cdots + g_s l_{s,s},$$

worin $g_s = L_{s-1}$ ist, und daher nach der gemachten Voraussetzung von Null verschieden angenommen werden kann. Substituiren wir diese Werthe von g in die Formel des Satzes 4, §. 185, indem wir $g_{s+1} = 0, \ldots, g_\nu = 0$ annehmen, während g_s nicht $= 0$ ist, so sind, so lange $s < \nu$ ist, gewiss nicht alle $g_1, g_2, \ldots, g_\nu$ einander gleich, und es ergiebt sich, dass sich ε_s so annehmen lässt, dass L_s von Null verschieden ist, wie bewiesen werden sollte.

Auf $s = \nu$ ist diese Schlussweise nicht auszudehnen, und die Determinante L_ν muss auch in der That immer Null sein, weil für jede Einheit $\sum\limits_{1,\nu}^{s} l_s$ verschwindet.

Wir wollen jetzt für den Fall, dass $s = \nu - 1$ ist, die Determinante L_s so bezeichnen:

(3)
$$L_{\nu-1} = L(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}),$$

und ein System von Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$, für welches diese Determinante von Null verschieden ist, ein System unabhängiger Einheiten nennen.

Der absolute Werth L der Determinante $L(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1})$ heisst der Regulator des Systems $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$[1].

Wenn wir in der Determinante

(4)
$$\begin{vmatrix} l_{1,1}, & l_{1,2}, & \ldots, l_{1,\nu} \\ \ldots & \ldots & \ldots \\ l_{\nu-1,1}, & l_{\nu-1,2}, & \ldots, l_{\nu-1,\nu} \\ x_1, & x_2, & \ldots, x_\nu \end{vmatrix},$$

in der die $x_1, x_2, \ldots, x_\nu$ willkürliche Grössen sind, alle Colonnen zu der letzten addiren, so erhalten wir mit Rücksicht auf die Relationen $\sum\limits^{i} l_{s,i} = 0$ ihren Werth gleich

$$\pm (x_1 + x_2 + \cdots + x_\nu)\, L.$$

Wenn wir also alle x mit Ausnahme von einem beliebigen

---

[1] Dirichlet-Dedekind, Vorlesungen über Zahlentheorie 4. Auflage, §. 183.

$= 0$, das eine $= 1$ annehmen, so ergiebt sich aus (3) irgend eine der $(\nu-1)$-reihigen Determinanten der Matrix

$$\begin{matrix} l_{1,1}, & l_{1,2}, & \ldots, l_{1,\nu} \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot \\ l_{\nu-1,1}, & l_{\nu-1,2}, & \ldots, l_{\nu-1,\nu} \end{matrix}$$

und alle diese Determinanten haben also (vom Vorzeichen abgesehen) denselben Werth. Es ist daher gleichgültig, welcher unter den ν conjugirten Werthen bei der Bildung des Regulators L weggelassen wird.

Ist $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ ein unabhängiges System von Einheiten, und sind $\lambda_1, \lambda_2, \ldots, \lambda_\nu$ die conjugirten Logarithmen irgend einer Einheit ε in Ω, so kann man die Zahlen $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ immer und nur auf eine Weise so bestimmen, dass

$$(5)\qquad \begin{aligned} \xi_1 l_{1,1} + \xi_2 l_{2,1} + \cdots + \xi_{\nu-1} l_{\nu-1,1} &= \lambda_1, \\ \xi_1 l_{1,2} + \xi_2 l_{2,2} + \cdots + \xi_{\nu-1} l_{\nu-1,2} &= \lambda_2, \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \xi_1 l_{1,\nu} + \xi_2 l_{2,\nu} + \cdots + \xi_{\nu-1} l_{\nu-1,\nu} &= \lambda_\nu \end{aligned}$$

wird. Denn von diesen Gleichungen sind die ersten $\nu - 1$ ein System linearer Gleichungen mit nicht verschwindender Determinante, und die ν^{te} Gleichung folgt aus den übrigen, weil die Summe der conjugirten Logarithmen einer jeden Einheit verschwindet.

Das System der Zahlen $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ nennen wir das Exponentensystem der Einheit ε in Bezug auf das System $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$, und es ist nun zu beweisen:

6. Dass die Exponenten jeder Einheit ε rationale Zahlen sind, deren Nenner eine gewisse endliche Grenze nicht übersteigt, und die daher alle mit einem gemeinschaftlichen, nur von dem Systeme ε_i abhängigen Nenner behaftet angenommen werden können.

Um dies einzusehen, hat man Folgendes zu erwägen:

1) Wenn wir die Grössen $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ wie Variable betrachten, und jede von ihnen, von den anderen unabhängig, von 0 bis 1 gehen lassen, so bleiben die linken Seiten von (5) in endlichen, nur von den Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ abhängigen Grenzen eingeschlossen. In diesen Grenzen müssen also auch die conjugirten Logarithmen λ der Einheit ε bleiben, so lange

die Exponenten ξ_i auf nicht negative echte gebrochene Werthe beschränkt bleiben, und daraus ergiebt sich nach der Definition der conjugirten Logarithmen eine obere Grenze für ε und seine Conjugirten.

Nach dem Satze 2., §. 185 giebt es aber in Ω nur eine endliche Anzahl ganzer Zahlen, also um so mehr nur eine endliche Anzahl von Einheiten, die dem absoluten Werthe nach mit allen ihren Conjugirten unter einer endlichen Grenze liegen.

Wenn wir nun eine Einheit, deren Exponenten in den Grenzen 0 und 1 liegen, mit Einschluss der unteren und mit Ausschluss der oberen Grenze eine in Bezug auf das System $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ reducirte Einheit nennen, so haben wir den Satz:

Es giebt nur eine endliche Anzahl von Einheiten in Ω, die in Bezug auf ein unabhängiges System $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ reducirt sind.

2) Die Einheiten reproduciren sich durch Multiplication und Division. Sind

$$\xi_1', \xi_2', \ldots, \xi_{\nu-1}'$$
$$\xi_1'', \xi_2'', \ldots, \xi_{\nu-1}''$$

die Exponenten von zwei Einheiten $\varepsilon', \varepsilon''$, so sind die Summen und die Differenzen

$$\xi_1' \pm \xi_1'', \xi_2' \pm \xi_2'', \ldots, \xi_{\nu-1}' \pm \xi_{\nu-1}''$$

die Exponenten der Einheiten $\varepsilon' \varepsilon''$ und $\varepsilon' : \varepsilon''$.

Dies ergiebt sich unmittelbar aus dem Satze, dass der Logarithmus eines Productes oder eines Quotienten gleich der Summe oder der Differenz der Logarithmen der beiden Bestandtheile ist.

3) Die Einheiten $\varepsilon_1, \varepsilon_2, \ldots$ selbst haben die Exponenten $1, 0, \ldots, 0$; $0, 1, \ldots, 0$; ..., und daraus folgt nach 2), dass jedes System von ganzen Zahlen, für $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ gesetzt, das Exponentensystem einer Einheit giebt, die sich durch Multiplication von Potenzen der $\varepsilon_1, \varepsilon_2, \ldots$ bilden lässt.

4) Aus 2) und 3) ergiebt sich, dass ein Exponentensystem $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ einer Einheit ein Exponentensystem bleibt, wenn alle seine Elemente mit einer und derselben ganzen Zahl multiplicirt werden, und dass es auch dann noch diesen Charakter behält, wenn seine Elemente ξ_i um beliebige ganze Zahlen vermehrt oder vermindert werden. Gebrauchen wir also das Zeichen (x) in dem Sinne, wie im §. 182, dass es den Ueber-

schuss der Zahl x über die grösste in x enthaltene ganze Zahl bedeutet, so ergiebt sich Folgendes:

Ist $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ das Exponentensystem einer Einheit, und m eine ganze Zahl, so ist auch

(6) $$(m\xi_1), (m\xi_2), \ldots, (m\xi_{\nu-1})$$

das Exponentensystem einer Einheit.

Nun sind die Grössen $(m\xi_i)$, wenn sie nicht Null sind, positive echte Brüche, und nach 1) muss es sich also, wenn die Reihe der ganzen Zahlen hinlänglich weit fortgesetzt wird, ereignen, dass für zwei verschiedene Werthe m', m'' von m die Zahlenreihe (6) übereinstimmt. Da hiernach $m'\xi_i$, $m''\xi_i$ denselben Ueberschuss über eine ganze Zahl haben, so ist $(m' - m'')\xi_i$ selbst eine ganze Zahl, und es giebt also eine ganze rationale Zahl m, die höchstens gleich der Anzahl der Exponentensysteme reducirter Einheiten ist, von der Eigenschaft, dass

$$m\xi_1, m\xi_2, \ldots, m\xi_{\nu-1}$$

ganze rationale Zahlen werden.

Diese Zahl m kann sich ändern, wenn die Einheit ε geändert wird. Da aber alle möglichen Werthe dieser Zahl unter einer endlichen Grenze liegen, so giebt es eine endliche Zahl, in der alle diese Werthe von m enthalten sind und die selbst für m genommen werden kann. Es giebt daher eine gewisse positive ganze Zahl m, die als Nenner aller der rationalen Zahlen genommen werden kann, die als Exponenten von Einheiten auftreten können. Damit ist der Satz 6. bewiesen.

§. 187.

Fundamentalsysteme von Einheiten.

Wir wählen jetzt an Stelle des Systemes unabhängiger Einheiten ε_i ein anderes, dessen conjugirte Logarithmen

(1) $$\lambda_{i,1}, \lambda_{i,2}, \ldots, \lambda_{i,\nu} \qquad i = 1, 2, \ldots, \nu - 1$$

sein mögen. Nach §. 186, (5) ist

(2) $$\lambda_{i,k} = \xi_{1,i} l_{1,k} + \xi_{2,i} l_{2,k} + \cdots + \xi_{\nu-1,i} l_{\nu-1,k}$$
$$i = 1, 2, \ldots, \nu - 1; \quad k = 1, 2, \ldots, \nu,$$

wenn $\xi_{1,i}, \xi_{2,i}, \ldots, \xi_{\nu-1,i}$ die Exponenten einer der neuen Einheiten in Bezug auf das System $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ bedeuten, die wir als rationale Zahlen mit dem gemeinsamen Nenner m annehmen können.

Es ist aber nach dem Multiplicationssatze der Determinanten

(3)
$$\begin{vmatrix} \lambda_{1,1}, & \ldots, & \lambda_{\nu-1,1} \\ \cdot & \cdot & \cdot \\ \lambda_{1,\nu-1}, & \ldots, & \lambda_{\nu-1,\nu-1} \end{vmatrix}$$
$$= \begin{vmatrix} \xi_{1,1}, & \ldots, & \xi_{1,\nu-1} \\ \cdot & \cdot & \cdot \\ \xi_{\nu-1,1}, & \ldots, & \xi_{\nu-1,\nu-1} \end{vmatrix} \begin{vmatrix} l_{1,1}, & \ldots, & l_{\nu-1,1} \\ \cdot & \cdot & \cdot \\ l_{1,\nu-1}, & \ldots, & l_{\nu-1,\nu-1} \end{vmatrix},$$

oder, wenn wir

$$\varDelta_{\nu-1} = \Sigma \pm \lambda_{1,1}\,\lambda_{2,2}\ldots\lambda_{\nu-1,\nu-1}$$

setzen, und beachten, dass die Determinante

$$\Sigma \pm \xi_{1,1}\,\xi_{2,2}\ldots\xi_{\nu-1,\nu-1}$$

eine rationale Zahl mit dem Nenner $m^{\nu-1}$ ist:

(4)
$$\varDelta_{\nu-1} = \frac{a}{m^{\nu-1}}\,L\,(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}),$$

worin a eine ganze rationale Zahl ist.

Daraus ergiebt sich, dass die neu eingeführten Einheiten immer und nur dann ein unabhängiges System bilden, wenn die Determinante der $\xi_{i,k}$, d. h. die Zahl a, von Null verschieden ist.

Nun giebt es unter einer endlichen oder unendlichen Anzahl nicht verschwindender rationaler Brüche mit demselben Nenner immer einen dem absoluten Werthe nach kleinsten, und folglich können wir nach (4) das neue System unabhängiger Einheiten so wählen, dass sein Regulator $\pm \varDelta_{\nu-1}$ so klein als möglich wird. Ein solches System nennen wir ein Fundamentalsystem von Einheiten, und den Minimalwerth des Regulators selbst, also den Regulator eines Fundamentalsystemes, nennen wir den Regulator des Körpers. Wir nehmen jetzt an, dass unser System $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ selbst ein Fundamentalsystem sei.

Unter dieser Voraussetzung lässt sich beweisen, dass alle Exponenten von Einheiten ganze Zahlen sein müssen.

Wenn wir nämlich annehmen, es existire eine Einheit ε, deren nach den Formeln §. 186, (5) bestimmte Exponenten nicht alle ganze Zahlen sind, so giebt es nach §. 186, 4) auch eine Einheit ε_0, deren Exponenten echte Brüche sind, die nicht alle verschwinden.

Verstehen wir unter $\lambda_1, \lambda_2, \ldots, \lambda_{\nu-1}$ in den Formeln (5), §. 186 das System der conjugirten Logarithmen von ε_0, so ergiebt sich

$$L\,(\varepsilon_0, \varepsilon_2, \ldots, \varepsilon_{\nu-1}) = \xi_1\,L\,(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}),$$

und wenn wir also annehmen, was offenbar keine Beschränkung der Allgemeinheit ist, dass ξ_1 ein nicht verschwindender echter Bruch sei, so widerspricht diese Formel der Annahme, dass

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$$

ein Fundamentalsystem sei, weil die Determinante $L_{\nu-1}$ verkleinert würde, wenn ε_1 durch ε_0 ersetzt wird.

Haben wir ein Fundamentalsystem, so können wir ein beliebiges System ganzer rationaler Zahlen $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ als Exponentensystem annehmen und eine Einheit ε mit diesen Exponenten bilden:

$$\varepsilon = \varepsilon_1^{\xi_1} \varepsilon_2^{\xi_2} \ldots \varepsilon_{\nu-1}^{\xi_{\nu-1}}.$$

Es bleibt also noch die Frage zu beantworten, inwieweit eine Einheit durch das Exponentensystem bestimmt ist.

Nehmen wir an, es seien ε', ε'' zwei Einheiten mit demselben Exponentensysteme, dann besteht das Exponentensystem der Einheit $\varepsilon' : \varepsilon'' = \varrho$ aus lauter Nullen, und folglich sind die conjugirten Logarithmen von ϱ alle gleich Null; ϱ ist daher eine ganze Zahl von der Eigenschaft, dass die absoluten Werthe aller mit ϱ conjugirten Zahlen gleich 1 sind, und daher, wie im §. 175, 2. bewiesen ist, eine Einheitswurzel. Damit ist das folgende Theorem bewiesen:

I. Es giebt im Körper Ω ein System von $\nu - 1$ fundamentalen Einheiten

(5) $$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1},$$

welches die Eigenschaft hat, dass in der Form

(6) $$\varepsilon = \varrho\, \varepsilon_1^{\xi_1} \varepsilon_2^{\xi_2} \ldots \varepsilon_{\nu-1}^{\xi_{\nu-1}}$$

alle Einheiten des Körpers, jede nur einmal, enthalten sind, wenn $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ alle ganzen rationalen Zahlen und ϱ alle in Ω vorhandenen Einheitswurzeln durchläuft.

Es ist nun leicht, aus einem Fundamentalsysteme alle anderen abzuleiten, indem man in (6) für die Exponenten $\nu - 1$ verschiedene Systeme ganzer Zahlen $\xi_{i,k}$ setzt, deren Determinante $= \pm 1$ ist. Denn setzt man

$$\varepsilon_i' = \varrho_i\, \varepsilon_1^{\xi_{1,i}} \varepsilon_2^{\xi_{2,i}} \ldots \varepsilon_{\nu-1}^{\xi_{\nu-1,i}},$$

so folgt aus (3):

$$L(\varepsilon_1', \varepsilon_2', \ldots, \varepsilon_{\nu-1}') = \pm L(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}).$$

Beide Determinanten haben also den Minimalwerth, und beide Systeme sind Fundamentalsysteme.

Der Fall $\nu = 1$, den wir oben ausgeschlossen haben, tritt ausser im Falle des rationalen Körpers, in dem nur die beiden Einheiten ± 1 existiren, im Falle des imaginären quadratischen Körpers ein. In diesem Falle haben wir im zwanzigsten Abschnitte die ganzen Zahlen des Körpers in der Form

$$\frac{x + y\sqrt{-m}}{2}$$

dargestellt, worin $-m$ eine Stammdiscriminante bedeutet, so dass $m \equiv 0$ oder $\equiv 3 \pmod 4$ ist, und x, y beide gerade oder beide ungerade sind. Die Einheiten erhalten wir, wenn wir die Gleichung

$$x^2 + my^2 = 4$$

auf alle mögliche Arten in ganzen rationalen Zahlen lösen. Diese Gleichung hat aber, wenn $m > 4$ ist, nur die zwei Lösungen $x = \pm 2$, $y = 0$, und es giebt also in diesen Fällen, wie im Körper der rationalen Zahlen, nur die zwei Einheiten ± 1. Ist $m = 4$, so findet man die vier Einheiten ± 1, $\pm i$, und ist endlich $m = 3$, die sechs Einheiten

$$\pm 1, \quad \pm \frac{-1 + i\sqrt{3}}{2}, \quad \pm \frac{-1 - i\sqrt{3}}{2}.$$

In dem nächst einfachen Falle, $n = 2$, $\nu = 2$, d. h. im reellen quadratischen Körper, fällt die Theorie der Einheiten zusammen mit der im §. 127 des ersten Bandes behandelten Theorie der Pell'schen Gleichung.

§. 188.

Reducirte Zahlen.

Ist α irgend eine von Null verschiedene ganze oder gebrochene Zahl des Körpers Ω, so betrachten wir, wie bei den Einheiten, das System der conjugirten Logarithmen von α, worunter wir, wie im §. 185, die reellen Zahlen

(1) $$\lambda_1 = \delta_1 \log|\alpha_1|, \; \lambda_2 = \delta_2 \log|\alpha_2|, \; \ldots, \; \lambda_\nu = \delta_\nu \log|\alpha_\nu|$$

verstehen, die wir auch mit $\lambda_s(\alpha)$ bezeichnen. Ziehen wir das Fundamentalsystem $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ von Einheiten zu Rathe, so

können wir die linearen Gleichungen, analog wie im §. 186, (5) bilden:

$$(2)\quad \begin{array}{l} \xi_1 l_{1,1} + \xi_2 l_{2,1} + \cdots + \xi_{\nu-1} l_{\nu-1,1} + \delta_1 \xi_\nu = \lambda_1, \\ \xi_1 l_{1,2} + \xi_2 l_{2,2} + \cdots + \xi_{\nu-1} l_{\nu-1,2} + \delta_2 \xi_\nu = \lambda_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \xi_1 l_{1,\nu} + \xi_2 l_{2,\nu} + \cdots + \xi_{\nu-1} l_{\nu-1,\nu} + \delta_\nu \xi_\nu = \lambda_\nu, \end{array}$$

dessen Determinante [§. 186, (4)] den von Null verschiedenen Werth hat:

$$(3)\quad \begin{vmatrix} l_{1,1}, & l_{2,1}, & \ldots, & l_{\nu-1,1}, & \delta_1 \\ l_{1,2}, & l_{2,2}, & \ldots, & l_{\nu-1,2}, & \delta_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ l_{1,\nu}, & l_{2,\nu}, & \ldots, & l_{\nu-1,\nu}, & \delta_\nu \end{vmatrix} = n\, L\,(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1})$$

Demnach sind die Unbekannten $\xi_1, \xi_2, \ldots, \xi_{\nu-1}, \xi_\nu$ aus (2) eindeutig bestimmt.

Durch Addition der Gleichungen (2) findet man zunächst sehr einfach

$$(4)\quad n\,\xi_\nu = \log N_a(\alpha),$$

und ξ_ν bleibt also dasselbe für alle Zahlen α, die unter einander associirt sind.

Die Zahlen $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ heissen die Exponenten der Zahl α [in Bezug auf das Fundamentalsystem $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1})$].

Aus dieser Definition ergiebt sich ohne Weiteres, dass die Exponenten eines Productes oder eines Quotienten gleich der Summe oder der Differenz der entsprechenden Exponenten der einzelnen Bestandtheile sind. Die Exponenten einer Einheit sind ganze rationale Zahlen, und jedes System ganzer rationaler Zahlen $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ ist auch das Exponentensystem einer Einheit.

Die Exponenten associirter Zahlen unterscheiden sich also um ganze Zahlen von einander, und man kann zu jeder Zahl α eine associirte Zahl α_0 finden, deren Exponenten zwischen 0 und 1 liegen. Solche Zahlen heissen reducirte Zahlen (in Bezug auf das Fundamentalsystem $\varepsilon_1, \ldots, \varepsilon_{\nu-1}$). Reducirte Einheiten sind alle und nur die in Ω vorhandenen Einheitswurzeln, deren Zahl wir mit w bezeichnen wollen. Da die beiden Einheitswurzeln ± 1 in jedem Körper enthalten sind, so ist w mindestens $= 2$ und immer eine gerade Zahl.

Wenn zwei associirte Zahlen dasselbe Exponentensystem haben, so unterscheiden sie sich nur durch einen Factor, der

eine Einheitswurzel ist. Das Exponentensystem der aus α abgeleiteten reducirten Zahl α_0 ist durch α selbst völlig bestimmt. Hierdurch ist der Satz bewiesen:

II. Zu jeder (von Null verschiedenen) Zahl α des Körpers Ω giebt es w und nicht mehr reducirte Zahlen $\varrho\alpha_0$.

Wenn statt des Fundamentalsystemes $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1})$ ein anderes angewendet wird, so erleiden die Exponenten $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ eine ganzzahlige lineare Substitution von der Determinante ± 1. Eine reducirte Zahl kann dann aufhören, für das neue Fundamentalsystem reducirt zu sein. Der Begriff der reducirten Zahl ist also von der Wahl des Fundamentalsystemes abhängig. Die Anzahl der aus einer gegebenen Zahl abgeleiteten reducirten Zahlen ist aber immer dieselbe.

Durch diesen Satz haben wir den Zweck erreicht, aus dem ganzen unendlichen Systeme der unter einander associirten Zahlen eine bestimmte endliche Anzahl von Repräsentanten herausgehoben zu haben.

§. 189.

Grenzen der Anzahl der durch ein Ideal theilbaren ganzen Zahlen des Körpers Ω.

Unsere früheren Betrachtungen haben ergeben, dass jede ganze Zahl eines Körpers Ω nur eine endliche Anzahl von Idealen zu Theilern hat. Da jedes ganze Ideal ein Theiler seiner Norm ist, so giebt es also auch nur eine endliche Anzahl von ganzen Zahlen in Ω, deren absolute Norm eine gegebene Grenze nicht übersteigt.

Aus diesen Zahlen greifen wir jetzt wieder einen Theil heraus, und fragen nach der Anzahl T aller ganzen Zahlen des Körpers Ω, deren absolute Norm eine positive Grösse t nicht überschreitet, und die durch ein gegebenes Ideal $\mathfrak{a}$ theilbar sind.

Nehmen wir als vorläufiges Beispiel den rationalen Körper, so ist dort T die Anzahl der natürlichen Zahlen, die kleiner als t und durch eine gegebene ganze Zahl m theilbar sind, also, in der früher (§. 182) gebrauchten Bezeichnung $T = E\left(\frac{t}{m}\right)$.

Die Zahl T ist eine im Allgemeinen nicht genauer zu bestimmende Function von t, die mit t zugleich ins Unendliche wächst, die sich aber, da sie nur ganzzahlige Werthe hat, nur stufenweise, also unstetig ändert. Worauf es hier ankommt, ist der Grenzwerth, dem sich das Verhältniss $T:t$ mit unendlich wachsendem t nähert (der in dem oben angeführten Beispiele $1:m$ ist).

Dieser Grenzwerth lässt sich durch Betrachtungen, wie wir sie schon im §. 155 benutzt haben, finden.

Wir bilden uns zunächst eine Basisform des gegebenen Ideals $\mathfrak{a}$:

(1) $$\alpha = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n,$$

d. h. eine lineare Function der n Variablen x_i, von der Eigenschaft, dass durch Substitution aller ganzen rationalen Zahlen für x_i aus α alle durch $\mathfrak{a}$ theilbare ganze Zahlen des Körpers Ω entstehen (§. 146). Mit $\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,n}$ bezeichnen wir die mit α_i conjugirten Werthe und bilden die lineare Substitution für x_i:

(2) $$\begin{aligned} y_1 &= \alpha_{1,1} x_1 + \alpha_{2,1} x_2 + \cdots + \alpha_{n,1} x_n \\ y_2 &= \alpha_{1,2} x_1 + \alpha_{2,2} x_2 + \cdots + \alpha_{n,2} x_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ y_n &= \alpha_{1,n} x_1 + \alpha_{2,n} x_2 + \cdots + \alpha_{n,n} x_n. \end{aligned}$$

Ist A die Determinante dieses Gleichungssystems

$$A = \Sigma \pm \alpha_{1,1}\alpha_{2,2}\ldots\alpha_{n,n},$$

so ist A^2 die Discriminante des Functionensystems $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, und daher nach §. 147 gleich dem Producte aus dem Quadrate der absoluten Norm von α und der Körperdiscriminante Δ. Da die absolute Norm von α zugleich die Norm des Ideals $\mathfrak{a}$ ist (§. 151), so setzen wir

(3) $$A^2 = N(\mathfrak{a})^2\,\Delta.$$

Nun können wir, wie im §. 155, die $x_1, x_2, \ldots, x_n$ als Coordinaten eines Punktes (x) in einem Raume von n Dimensionen deuten, und wir lassen jedem Punkt (x) einen Punkt (x') entsprechen, dessen Coordinaten durch

(4) $$x_1' = t^{\frac{1}{n}} x_1,\quad x_2' = t^{\frac{1}{n}} x_2,\ \ldots,\ x_n' = t^{\frac{1}{n}} x_n$$

bestimmt sind, worin t eine beliebige positive Grösse bedeutet. Jedem Gebiete S von Punkten (x) entspricht ein Gebiet S' von Punkten (x'). Alle Figuren in S sind den entsprechenden Figuren in S' ähnlich, und die Lineardimensionen in S verhalten sich zu denen in S' wie $1:t^{\frac{1}{n}}$.

Denken wir uns das Gebiet S gegeben, so wird das entsprechende Gebiet S' von t abhängig sein und sich mit t vergrössern. Die Punkte mit ganzzahligen Coordinaten x_i nennen wir, wie früher, die Gitterpunkte. Die Anzahl der in einem endlichen Gebiete S' liegenden Gitterpunkte ist immer endlich, wächst aber mit t und soll mit Z_t bezeichnet werden. Dann ist nach den Sätzen §. 155, (14) das Volumen des Gebietes S, d. h. das über alle Punkte von S erstreckte n-fache Integral

$$V = \int\int \dots \int d x_1\, d x_2 \dots d x_n$$

gleich dem Grenzwerthe des Verhältnisses $Z_t : t$ für unendlich wachsendes t:

(5) $$V = \lim_{t = \infty} \frac{Z_t}{t}.$$

Hierin liegt zugleich die genauere Präcisirung, die wir über das Gebiet S machen müssen, wenn unsere Betrachtung anwendbar sein soll. Es muss S so beschaffen sein, dass das n-fache Integral V eine bestimmte Bedeutung hat. Jeder Gitterpunkt ist nun durch (1) das Bild einer ganzen durch $\mathfrak{a}$ theilbaren Zahl des Körpers Ω, und wir können also auch sagen, dass Z_t die Anzahl der durch $\mathfrak{a}$ theilbaren ganzen Zahlen in Ω ist, deren Bilder in dem Gebiete S' liegen.

Um das Gebiet S' in geeigneter Weise abzugrenzen, wählen wir ein System fundamentaler Einheiten des Körpers Ω

$$\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\nu-1}$$

mit dem System der conjugirten Logarithmen

$$l_{i,1}, l_{i,2}, \dots, l_{i,\nu}$$

und dem Regulator

(6) $$\pm L(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\nu-1}) = \pm \Sigma \pm l_{1,1}\, l_{2,2} \dots l_{\nu-1,\nu-1},$$

der mit L bezeichnet werden mag.

Wir definiren jetzt ein System von Functionen $\xi_1, \xi_2, \dots, \xi_\nu$ der Variablen x_i durch folgende Bedingungen:

Es sei, wenn die y_i die Bedeutung (2) haben,

(7) $$z_i = \delta_i \log |y_i|,$$

so dass, wenn für die x_i ein System ganzer rationaler Zahlen gesetzt wird, z_i nach §. 185 in das System der conjugirten Logarithmen der Zahl α übergeht.

Es ist dann, wenn y_k zu einem reellen Körper gehört,

(8) $$z_k = \tfrac{1}{2} \log y_k^2,$$

und wenn y_k, y'_k einem imaginären Paare angehören,

(9) $$z_k = \log y_k\, y'_k,$$

wodurch die Definition völlig eindeutig ist.

Nun bestimmen wir die Variablen $\xi_1, \xi_2, \ldots, \xi_{\nu-1}, \xi_\nu$ aus den linearen Gleichungen

(10) $$\begin{array}{l} \xi_1\, l_{1,1} + \cdots + \xi_{\nu-1}\, l_{\nu-1,1} + \delta_1\, \xi_\nu = z_1 \\ \xi_1\, l_{1,2} + \cdots + \xi_{\nu-1}\, l_{\nu-1,2} + \delta_2\, \xi_\nu = z_2 \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ \xi_1\, l_{1,\nu} + \cdots + \xi_{\nu-1}\, l_{\nu-1,\nu} + \delta_\nu\, \xi_\nu = z_\nu, \end{array}$$

deren Determinante nicht verschwindet.

Giebt man den Variablen x_i ganzzahlige Werthe, so gehen nach §. 188, (2), (3) die $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ in das Exponentensystem der Zahl α über, und es ergiebt sich durch Addition der Gleichungen (10) [§. 185, (3)]:

(11) $$\xi_\nu = \frac{1}{n} \log N_a(\alpha).$$

Wir gehen jetzt von dem Punkte (x) zu dem Punkte (x') über, indem wir $x'_i = t^{\frac{1}{n}} x_i$ setzen. Dadurch geht y_i in

$$y'_i = t^{\frac{1}{n}} y_i$$

über, und z_i in

$$z'_i = z_i + \frac{1}{n}\, \delta_i \log t.$$

Wenn wir also z'_i an Stelle von z_i setzen, und die dann aus (10) sich ergebenden Werthe der $\xi_1, \xi_2, \ldots, \xi_\nu$ mit $\xi'_1, \xi'_2, \ldots, \xi'_\nu$ bezeichnen, so ist

(12) $$\xi'_1 = \xi_1,\ \xi'_2 = \xi_2, \ldots, \xi'_{\nu-1} = \xi_{\nu-1},\ \xi'_\nu = \xi_\nu + \frac{1}{n} \log t.$$

Nunmehr wollen wir das Gebiet S' dadurch abgrenzen, dass

(13) $$\begin{array}{c} 0 \gtreqless \xi'_1 < 1, \ldots, 0 \gtreqless \xi'_{\nu-1} < 1, \\ \xi'_\nu < \dfrac{1}{n} \log t \end{array}$$

sein soll. Dadurch erreichen wir, dass die in dem Gebiete S' liegenden Gitterpunkte (x') nur reducirte ganze Zahlen α darstellen, und alle und nur solche, deren absolute Norm kleiner als t ist.

Unter den reducirten Zahlen sind aber immer je w mit einander associirt, wenn w die Anzahl der in Ω enthaltenen

Einheitswurzeln bedeutet, und wenn wir also diese w associirten Zahlen zu einem Complex zusammenfassen, so ist die Anzahl dieser Complexe gleich der Anzahl T aller nicht associirten, durch $\mathfrak{a}$ theilbaren ganzen Zahlen in Ω, deren absolute Norm kleiner als t ist. Demnach ist die Anzahl der in S' liegenden Gitterpunkte

$$(14) \qquad Z_t = w\,T.$$

Für die Begrenzung des Gebietes S erhält man aus (12) und (13):

$$(15) \qquad 0 \gtreqless \xi_1 < 1, \ldots, 0 \gtreqless \xi_{\nu-1} < 1, \; \xi_\nu < 0,$$

und nach (5) erhalten wir

$$(16) \qquad \operatorname{Lim} \frac{T}{t} = \frac{1}{w} \int\!\!\int \ldots \int d x_1\, d x_2 \ldots d x_n = \frac{1}{w}\, V,$$

worin das n-fache Integral über das durch (15) bestimmte Gebiet S auszudehnen ist.

§. 190.

Bestimmung des Volumens.

Das Volumen V lässt sich bestimmen nach der schon im §. 155 angeführten Transformationsformel für mehrfache Integrale, nach der, wenn $x_1, x_2, \ldots, x_n$ Functionen der Variablen $u_1, u_2, \ldots, u_n$ sind,

$$(1) \qquad V = \int\!\!\int \ldots \int d x_1\, d x_2 \ldots d x_n$$
$$= \int\!\!\int \ldots \int \left(\Sigma \pm \frac{\partial x_1}{\partial u_1} \frac{\partial x_2}{\partial u_2} \cdots \frac{\partial x_n}{\partial u_n} \right) d u_1\, d u_2 \ldots d u_n$$

ist, wobei die Functionaldeterminante in dem nach den Variablen u genommenen Integrale mit ihrem absoluten Werthe zu nehmen ist.

Diese Functionaldeterminante ist auch gleich dem reciproken Werthe der Determinante

$$\Sigma \pm \frac{\partial u_1}{\partial x_1} \frac{\partial u_2}{\partial x_2} \cdots \frac{\partial u_n}{\partial x_n}.$$

Wir führen zunächst die Variablen u durch eine lineare Substitution ein, und bemerken, dass unter den mit Ω conjugirten Körpern nach unserer Annahme $n - \nu$ conjugirt imaginäre Paare

und $2\nu - n$ reelle vorkommen. Demnach sind von den n Functionen y [§. 189, (2)]

(2) $$y_k = \alpha_{1,k} x_1 + \alpha_{2,k} x_2 + \cdots + \alpha_{n,k} x_n$$

$2\nu - n$ reell, $2n - 2\nu$ paarweise conjugirt. Wir wollen unter den n Variablen u reelle lineare Verbindungen der x verstehen, nämlich die $2\nu - n$ reellen y und die $2n - 2\nu$ Bestandtheile der conjugirt imaginären Paare der y, so dass, wenn y, y' ein imaginäres Paar ist,

$$2u_1 = y + y', \quad 2iu_2 = y - y'$$

oder

(3) $$y = u_1 + iu_2, \quad y' = u_1 - iu_2$$

gesetzt wird. Wenn man in der Functionaldeterminante der y auf jedes Paar conjugirt imaginärer Zeilen zweimal den elementaren Determinantensatz von der Addition der Zeilen anwendet (Bd. I, §. 22), so ergiebt sich

$$\Sigma \pm \frac{\partial u_1}{\partial x_1} \frac{\partial u_2}{\partial x_2} \cdots \frac{\partial u_n}{\partial x_n} =$$

$$\frac{1}{(-2i)^{n-\nu}} \Sigma \pm \frac{\partial y_1}{\partial x_1} \frac{\partial y_2}{\partial x_2} \cdots \frac{\partial y_n}{\partial x_n} = \frac{A}{(-2i)^{n-\nu}},$$

worin A die in §. 189, (3) festgesetzte Bedeutung hat.

Die Körperdiscriminante ist positiv oder negativ, je nachdem die Anzahl der conjugirt imaginären Paare, also $n - \nu$, gerade oder ungerade ist, und demnach erhält man, wenn mit $\pm \Delta$ der absolute Werth der Körperdiscriminante bezeichnet wird, nach §. 189, (4), (16):

(4) $$\operatorname{Lim} \frac{T}{t} = \frac{2^{n-\nu}}{w N(\mathfrak{a}) \sqrt{\pm \Delta}} \int\int \cdots \int du_1\, du_2 \ldots du_n.$$

Es ist also weiter noch das Integral

$$U = \int\int \cdots \int du_1\, du_2 \ldots du_n$$

zu behandeln.

Aus den Gleichungen §. 189, (10) erhält man zu jedem den Bedingungen (15) genügenden Werthsysteme der Variablen $\xi_1, \xi_2, \ldots, \xi_\nu$ ein bestimmtes endliches System der Werthe für $z_1, z_2, \ldots, z_\nu$, und daraus nach §. 189, (7) für jedes y einen von Null verschiedenen absoluten Werth. Setzt man im Falle eines imaginären Paares (3)

(5) $$u_1 = e^{1/2 z} \cos \vartheta, \quad u_2 = e^{1/2 z} \sin \vartheta,$$

(6) $$y_1 y_1' = u_1^2 + u_2^2 = e^z,$$

so ergiebt sich, wenn ϑ in den Grenzen

$$0 \leqq \vartheta < 2\pi$$

genommen wird, bei feststehendem z zu jedem Werthe von ϑ ein zugehöriges Werthepaar u_1, u_2. Ein solcher Winkel ϑ gehört zu jedem imaginären Paare.

Es gehört dann zu jedem Punkte des Gebietes S ein und nur ein Werthsystem der Variablen $\xi_1, \xi_2, \ldots, \xi_\nu, \vartheta \ldots$ in der Begrenzung

$$(7) \qquad 0 \gtreqless \xi_1 < 1, \ldots, 0 \gtreqless \xi_{\nu-1} < 1$$
$$\xi_\nu < 0, \qquad 0 \leqq \vartheta < 2\pi, \ldots$$

Wenn umgekehrt irgend ein Werthsystem der Variablen ξ, ϑ in den Grenzen (7) gegeben ist, so erhält man hieraus die entsprechenden Bestandtheile u_1, u_2 eines imaginären y eindeutig, von den reellen y aber nur die absoluten Werthe, und es kann also jedem der reellen y noch jedes der beiden Vorzeichen gegeben werden. Die Anzahl dieser möglichen Bestimmungen ist $2^{2\nu-n}$. Ist eine dieser Bestimmungen herausgegriffen, so sind die Variablen x eindeutig bestimmt und sind für jedes endliche Werthsystem der ξ, ϑ endlich. Für ein gegen $-\infty$ abnehmendes ξ_ν werden die Werthe der y zum Theil gegen Null convergiren.

Das Gebiet S zerfällt demnach in $2^{2\nu-n}$ Theilgebiete $S_1, S_2, \ldots$, deren jedes durch eine bestimmte Vorzeichen-Combination der reellen $y_1, y_2, \ldots$ charakterisirt ist, und demnach zerfällt das Integral U in ebenso viele Theilintegrale $U_1, U_2, \ldots$

$$U = U_1 + U_2 + \cdots$$

Bei der Ausführung der Integration in einem dieser Bestandtheile, die sich alle als von gleichem Werthe ergeben, fangen wir mit einem imaginären Paare an, wenn ein solches vorhanden ist.

Betrachten wir u_1, u_2 als rechtwinkelige Coordinaten in einer Ebene, so können wir $e^{1/2 z}, \vartheta$ nach (5) als Polarcoordinaten auffassen, und erhalten

$$\int\!\!\int du_1\, du_2 = \tfrac{1}{2}\int\!\!\int e^z\, dz\, d\vartheta,$$

worin die Integration in Bezug auf ϑ, die sich von 0 bis 2π erstreckt, ausgeführt werden kann. Man findet so

$$\int\!\!\int du_1\, du_2 = \pi \int e^z\, dz.$$

Nun ändert man die Reihenfolge der Integration, und stellt n etwa noch vorhandenes zweites imaginäres Paar voran, das an wieder in derselben Weise behandelt.

Die verschiedenen Bestandtheile $U_1, U_2, \ldots$ unterscheiden :h durch die Vorzeichen der den reellen y entsprechenden u. ehmen wir das Zeichen so, dass $\pm u$ positiv wird, und setzen

) $$z = \log(\pm u), \quad \pm du = e^z dz,$$

erhalten wir für die verschiedenen $U_1, U_2, \ldots$ denselben Aus-'uck durch ein ν-faches Integral

) $$U_1 = \pi^{n-\nu} \int\int \ldots \int e^{z_1 + z_2 + \cdots + z_\nu} dz_1\, dz_2 \ldots dz_\nu,$$

ənn wir $dz_1, dz_2, \ldots, dz_\nu$ positiv annehmen.

Die Variablen z_k sind aber nach (6) und (8) hier keine .deren, als in §. 189, (8), (9), (10), und danach ist

$$z_1 + z_2 + \cdots + z_\nu = n\,\xi_\nu.$$

Wenn wir nun die Transformationsformel (1) auf das ν-fache tegral (9) anwenden, um die Variablen $\xi_1, \xi_2, \ldots, \xi_\nu$ einzu-hren, so haben wir die Determinante

$$\Sigma \pm \frac{\partial z_1}{\partial \xi_1} \frac{\partial z_2}{\partial \xi_2} \cdots \frac{\partial z_\nu}{\partial \xi_\nu}$$

bilden, die nach §. 188, (3) dem absoluten Werthe nach mit L, d. h. mit dem $n$fachen Werthe des Körperregulators L ereinstimmt, und danach ist

$$U_1 = \pi^{n-\nu} n L \int_0^1 d\xi_1 \ldots \int_0^1 d\xi_{\nu-1} \int_{-\infty}^0 e^{n\xi_\nu} d\xi_\nu = \pi^{n-\nu} L$$

d

$$U = 2^{2\nu - n} \pi^{n-\nu} L.$$

.raus ergiebt sich also endlich nach (4) der Satz:

1. **Bedeutet T die Anzahl der durch $\mathfrak{a}$ theilbaren nicht associirten ganzen Zahlen, deren absolute Norm kleiner als t ist, so ist**

) $$\lim_{t=\infty} \frac{T}{t} = \frac{2^\nu \pi^{n-\nu} L}{w N(\mathfrak{a}) \sqrt{\pm \Delta}} = \frac{g}{N(\mathfrak{a})},$$

worin g eine durch die Natur des Körpers Ω völlig bestimmte positive Zahl ist, nämlich:

) $$g = \frac{2^\nu \pi^{n-\nu} L}{w \sqrt{\pm \Delta}}.$$

§. 191.

Sätze aus der Reihenlehre.

Bei den weiteren Anwendungen der bisherigen Resultate sind einige Sätze aus der Lehre von den unendlichen Reihen erforderlich, die zunächst hier abgeleitet werden sollen.

1. **Ist $a_1, a_2, a_3, \ldots, a_n \ldots$ ein unbegrenztes System reeller (positiver, negativer oder auch verschwindender) Grössen, von dem wir voraussetzen, dass die Summe**

(1) $$\sigma_n = a_1 + a_2 + \cdots + a_n$$

für jedes beliebige n dem absoluten Werthe nach unter einer endlichen Grenze C bleibt, so ist die Reihe

(2) $$S = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \cdots$$

für jedes positive s nicht nur convergent, sondern auch eine stetige Function von s.

Um diesen Satz zu beweisen, zerlegen wir S in der Weise:

$$S = S_m + R_m,$$

worin

$$S_m = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \cdots + \frac{a_{m-1}}{(m-1)^s},$$

$$R_m = \frac{a_m}{m^s} + \frac{a_{m+1}}{(m+1)^s} + \frac{a_{m+2}}{(m+2)^s} + \cdots$$

Nun ist nach (1):

$$a_m = \sigma_m - \sigma_{m-1},\ a_{m+1} = \sigma_{m+1} - \sigma_m,\ a_{m+2} = \sigma_{m+2} - \sigma_{m+1}, \ldots$$

und daher

$$R_m + \frac{\sigma_{m-1}}{m^s} = \sigma_m \left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right)$$
$$+ \sigma_{m+1}\left(\frac{1}{(m+1)^s} - \frac{1}{(m+2)^s}\right) + \cdots$$

Da nun nach der Voraussetzung $\sigma_{m-1}, \sigma_m, \sigma_{m+1}, \ldots$ zwischen endlichen Grenzen $\pm C$ eingeschlossen sind, so ist hiernach $R_m + \frac{\sigma_{m-1}}{m^s}$ zwischen den beiden Grenzen

$$\pm C\left(\frac{1}{m^s} - \frac{1}{(m+1)^s} + \frac{1}{(m+1)^s} - \frac{1}{(m+2)^s} + \cdots\right) = \pm \frac{C}{m^s}$$

eingeschlossen, und es ist dem absoluten Werthe nach

$$R_m < \frac{2\,C}{m^s},$$

oder, wenn $s > c$ ist,

$$R_m < \frac{2\,C}{m^c}.$$

Diese obere Grenze für R_m, die von s unabhängig ist, kann aber, wenn c positiv ist, dadurch, dass man m hinlänglich gross annimmt, unter jeden noch so kleinen Werth herabgedrückt werden.

Daraus folgt aber nicht nur die Convergenz, sondern auch die Stetigkeit von S. Denn nimmt man m hinlänglich gross, so wird nicht nur R_m, sondern es werden auch die Schwankung von R_m bei veränderlichem s unendlich klein, und S_m ist für ein feststehendes m eine stetige Function von s. Also ist auch S stetig.

Es ist dabei noch zu bemerken, dass die Voraussetzung über σ_m keineswegs die Convergenz der unendlichen Reihe $\Sigma\, a_k$ voraussetzt. Es ist nicht einmal erforderlich, dass die a_k reell seien; denn wenn sie imaginär sind, so braucht man nur den Satz auf den reellen und den imaginären Bestandtheil anzuwenden. Endlich ist es auch nicht nothwendig, die $a_1, a_2, a_3, \ldots$ als Constanten vorauszusetzen. Alles bleibt gültig, wenn es stetige Functionen von s sind.

2. Bedeutet $\mu_1, \mu_2, \ldots, \mu_n, \ldots$ eine unendliche Menge positiver Zahlen von der Beschaffenheit, dass zwei endliche Zahlen α, β so angegeben werden können, dass für jedes noch so grosse n

(3) $$\alpha < \frac{n}{\mu_n} < \beta,$$

so ist die unendliche Reihe

$$S = \frac{1}{\mu_1^s} + \frac{1}{\mu_2^s} + \frac{1}{\mu_3^s} + \cdots$$

convergent, so lange der Exponent s grösser als 1 ist, und das Product $(s-1)\,S$ bleibt bei hinlänglicher Annäherung von s an den Werth 1 gleichfalls zwischen den Grenzen α und β oder nähert sich wenigstens einem dieser Werthe unbegrenzt an.

Der Beweis ist durch Zurückführung auf ein Integral sehr einfach zu führen. Offenbar ist nämlich

$$\frac{1}{(n+1)^s} < \int\limits_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s},$$

weil sich der erste oder der zweite Werth, $(n+1)^{-s}$ oder n^{-s}, ergiebt, wenn unter dem Integralzeichen für x^{-s} der zu kleine oder der zu grosse Werth $(n+1)^{-s}$ oder n^{-s} gesetzt wird.

Demnach ergiebt sich aus (3) für jedes positive s

$$\alpha^s \int\limits_n^{n+1} \frac{dx}{x^s} < \frac{1}{\mu_n^s} < \beta^s \int\limits_{n-1}^{n} \frac{dx}{x^s}.$$

Setzen wir

$$R_m = \frac{1}{\mu_{m+1}^s} + \frac{1}{\mu_{m+2}^s} + \frac{1}{\mu_{m+3}^s} + \cdots,$$

so ergiebt sich hieraus

$$\alpha^s \int\limits_{m+1}^{\infty} \frac{dx}{x^s} < R_m < \beta^s \int\limits_{m}^{\infty} \frac{dx}{x^s}$$

oder

$$(4) \qquad \frac{\alpha^s}{(s-1)(m+1)^{s-1}} < R_m < \frac{\beta^s}{(s-1)\, m^{s-1}}.$$

Es bleibt also R_m, wie viele Glieder auch summirt werden mögen, wenn $s > 1$ ist, endlich, und dies ist bei Reihen mit positiven Gliedern eine ausreichende Bedingung für die Convergenz.

Setzt man ferner (4) in die Form

$$\frac{\alpha^s}{(m+1)^{s-1}} < (s-1)\, R_m < \frac{\beta^s}{m^{s-1}},$$

so sieht man, dass die beiden Grenzen beliebig nahe an α, β gebracht werden können, wenn man $s-1$ klein genug annimmt, und daraus ergiebt sich, dass $(s-1)\, R_m$ bei hinlänglich kleinem $s-1$ nicht mehr ausserhalb der Grenzen α, β liegen kann, wenn es sich nicht mit abnehmendem $s-1$ einem dieser Werthe unbegrenzt annähert. Da sich nun R_m von S nur durch einen Bestandtheil unterscheidet, der für jedes positive s endlich ist, so ist der Satz hiermit bewiesen.

Es gilt der Satz aber auch dann noch, wenn die Ungleichheit (3) nicht für alle n gilt, sondern wenn sie nur besteht, sobald n eine beliebig gegebene Grenze m überschritten hat. Auf

Grund dieser Bemerkung kann man, wenn sich $n : \mu_n$ einem endlichen Grenzwerthe γ nähert, α und β diesem Grenzwerthe beliebig nahe annehmen, und erhält so die etwas präcisere Fassung des Theorems:

3. Sind die positiven Zahlen $\mu_1, \mu_2, \mu_3, \ldots$ so beschaffen, dass

$$\lim_{n=\infty} \frac{n}{\mu_n} = \gamma$$

ein endlicher Grenzwerth ist, so ist die unendliche Reihe

$$S = \frac{1}{\mu_1^s} + \frac{1}{\mu_2^s} + \frac{1}{\mu_3^s} + \cdots$$

für jedes s, was grösser als 1 ist, convergent, und es ist

$$\lim_{s=1} (s-1)\, S = \gamma.$$

Es sei jetzt irgend ein System M von unendlich vielen positiven Zahlen μ_n gegeben, die wir so ordnen

$$(5) \qquad \mu_1 \gtreqless \mu_2 \gtreqless \mu_3 \gtreqless \cdots \qquad (M),$$

so dass in der Reihe (5) niemals ein kleineres Glied auf ein grösseres folgt, und es bedeute T die Anzahl von Gliedern in M, die nicht grösser als eine beliebig gegebene positive Grösse t sind. Es gilt dann folgender Satz:

4. Wenn einer der beiden Grenzwerthe

$$(6) \qquad \lim_{n=\infty} \frac{n}{\mu_n}, \quad \lim_{t=\infty} \frac{T}{t}$$

endlich ist, so hat der andere denselben endlichen Werth.

Es sei zunächst

$$(7) \qquad \lim_{n=\infty} \frac{n}{\mu_n} = \gamma$$

ein endlicher Grenzwerth. Dann werden die μ_n mit unendlich wachsendem n nothwendig ins Unendliche wachsen müssen, und es giebt für jedes positive t einen Werth m, so dass

$$(8) \qquad \mu_m \leqq t < \mu_{m+1};$$

m wächst zugleich mit t ins Unendliche und es ist $T = m$ [wegen (5)]. Daher nach (8)

$$(9) \qquad \frac{m}{\mu_m} \gtreqless \frac{T}{t} > \frac{m}{\mu_{m+1}}.$$

Wenn nun $\gamma = 0$ ist, so folgt hieraus, indem man t und m ins Unendliche wachsen lässt, dass auch $T : t$ den Grenzwerth 0 hat. Ist aber γ von 0 verschieden, so ist nach (7)

$$\text{Lim} \frac{\mu_m}{\mu_{m+1}} = \text{Lim} \frac{m}{m+1} = 1,$$

und daher nähern sich die beiden Grenzwerthe in (9) dem Werthe γ, und es folgt also:

$$\text{(10)} \qquad \text{Lim}_{t=\infty} \frac{T}{t} = \gamma.$$

Setzen wir zweitens umgekehrt die Grenzgleichung (10) voraus, so wird auch jetzt μ_n mit n ins Unendliche wachsen müssen, denn sonst würde, da die Gesammtzahl aller μ unendlich ist, T schon für ein endliches t unendlich, und γ könnte nicht endlich sein.

Nehmen wir nun einen Werth μ_n, der in der Reihe der unter einander gleichen

$$\mu_{m+1}, \mu_{m+2}, \ldots, \mu_{m+l}$$

vorkommt, so dass

$$m + 1 \lesseqgtr n \lesseqgtr m + l,$$

so wird T, wenn t durch den Werth μ_n geht, plötzlich um l Einheiten wachsen, und das Verhältniss $T : t$ wächst um $l : \mu_n$. Da aber $T : t$ einen endlichen Grenzwerth haben soll, so muss

$$\text{(11)} \qquad \text{Lim} \frac{l}{\mu_n} = 0$$

sein. Wenn nun $t = \mu_n$ ist, so ist $T = m + l$, und folglich ist

$$\text{(12)} \qquad \frac{T}{t} = \frac{m+l}{\mu_n}, \quad \text{Lim} \frac{m+l}{\mu_n} = \gamma.$$

Ferner

$$\frac{m}{\mu_n} < \frac{n}{\mu_n} \leqq \frac{m+l}{\mu_n},$$

und folglich ist wegen (11) und (12)

$$\text{Lim} \frac{n}{\mu_n} = \text{Lim} \frac{m}{\mu_n} = \gamma.$$

Also ist aus der Gleichung (10) die Gleichung (7) gefolgert [1]).

Mit Benutzung des Satzes 4. können wir nun dem Satze 3. auch die Form geben:

---

[1]) Dieser Satz ist im Wesentlichen auf dieselbe Weise bewiesen bei Dirichlet-Dedekind, Supplement II. Vgl. auch Riemann's mathematische Werke, 2. Auflage, Nr. XXX.

5. Ist T die Anzahl der Grössen μ_n, die nicht grösser als t sind, so ist

13) $$\operatorname*{Lim}_{s=1} \sum_{1,\infty}^{n} \frac{s-1}{\mu_n^{s-1}} = \operatorname*{Lim}_{t=\infty} \frac{T}{t},$$

wenn der Grenzwerth von $T:t$ endlich ist.

Nehmen wir an, dass die Grössen $\mu_1, \mu_2, \mu_3, \ldots$ nicht nur en Bedingungen des Satzes 3., sondern noch den weiteren enügen, dass, wenn

14) $$\mu_n = \frac{n + c_n}{\gamma}$$

esetzt wird, die c_n mit unendlich wachsendem n nicht unendlich rerden (d. h. für jedes noch so grosse n zwischen endlichen renzen eingeschlossen sind), so können wir den Satz 3. durch en noch schärferen ersetzen:

6. Haben die Zahlen μ_n die Eigenschaft, dass sich ein endliches γ so bestimmen lässt, dass

15) $$\gamma \mu_n - n = c_n$$

mit unendlich wachsendem n nicht unendlich wird, so hat die für jedes $s > 1$ definirte Function von s

16) $$S = \frac{1}{\mu_1^s} + \frac{1}{\mu_2^s} + \cdots$$

die Eigenschaft, dass die Differenz

17) $$S - \frac{\gamma}{s-1} = C_s$$

sich mit unendlich abnehmendem $s-1$ einer endlichen Grenze nähert.

Um dies zu beweisen, setzen wir nach (14) und (16):

18) $$\sum^{n} \frac{\gamma^s}{n^s} - S = \gamma^s \sum^{n} \frac{1}{n^s} \left[1 - \left(1 + \frac{c_n}{n}\right)^{-s}\right].$$

Wenn nun ε ein positiver echter Bruch ist, so ist, wenn wir

$$a_n = \frac{1}{n^\varepsilon} \left[1 - \left(1 + \frac{c_n}{n}\right)^{-s}\right]$$

etzen, $a_n n^{1+\varepsilon}$ für ein unendlich wachsendes n nicht unendlich, ind folglich ist nach einem bekannten elementaren Satze der Reihenlehre $a_1 + a_2 + \cdots$ eine unbedingt convergente Reihe.

Setzen wir nun

$$s = s_1 + \varepsilon,$$

so ergiebt sich aus (18):

$$\Sigma \frac{\gamma^s}{n^s} - S = \gamma^s \Sigma \frac{a_s}{n^{s_1}},$$

und dies ist nach 1. eine für positive s_1 endliche und stetige Function von s_1. Für $s_1 = 1 - \varepsilon$ wird aber $s = 1$, und folglich ist

(19) $$\Sigma \frac{\gamma^s}{n^s} - S = D_s$$

für $s = 1$ endlich, nämlich gleich

$$D_1 = \Sigma \frac{\gamma c_n}{n(n + c_n)}.$$

Mit Anwendung einfacher Sätze aus der Theorie der Γ-Functionen lässt sich aber die Summe $\Sigma \frac{1}{n^s}$ durch ein bestimmtes Integral ausdrücken. Es ist

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty e^{-nx} x^{s-1} dx,$$

und folglich

$$\Sigma \frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty \frac{x^{s-1} e^{-x} dx}{1 - e^{-x}}.$$

Ferner ist [nach dem Satze $(s-1)\Gamma(s-1) = \Gamma(s)$]:

$$\frac{1}{s-1} = \frac{1}{\Gamma(s)} \int_0^\infty e^{-x} x^{s-2} dx,$$

und daraus

$$\Sigma \frac{1}{n^s} - \frac{1}{s-1} = \frac{1}{\Gamma(s)} \int_0^\infty x^{s-1} e^{-x} \left(\frac{1}{1 - e^{-x}} - \frac{1}{x}\right) dx.$$

Hierin ist die rechte Seite eine für alle positiven Werthe von s stetige Function, die für $s = 1$ in die Euler'sche Constante

$$\int_0^\infty e^{-x} \left(\frac{1}{1 - e^{-x}} - \frac{1}{x}\right) dx = -\Gamma'(1) = 0{,}57721566\ldots$$

übergeht. Nun ist nach (19):

$$D_s = \gamma^s \left(\Sigma \frac{1}{n^s} - \frac{1}{s-1}\right) - \left(S - \frac{\gamma_s}{s-1}\right),$$

und daher

(20) $$\lim_{s=1}\left(S - \frac{\gamma_s}{s-1}\right) = -\gamma\Gamma'(1) + D_1 = C_1,$$

wie zu beweisen war, endlich[1]).

§. 192.

Anwendung auf die Bestimmung der Classenzahl.

Wir machen von diesen Sätzen jetzt die Anwendung auf die Theorie des Körpers Ω. Wir verstehen unter den Zahlen μ_n des Theorems 5. die Normen der sämmtlichen Ideale des Körpers Ω, also unter T die Anzahl der Ideale in Ω, deren Norm nicht grösser als eine gegebene positive Grösse t ist, und erhalten

(1) $$\lim_{s=1}\sum\frac{s-1}{N(\mathfrak{a})^s} = \lim_{t=\infty}\frac{T}{t},$$

und darin erstreckt sich die Summe der linken Seite auf alle Ideale $\mathfrak{a}$ des Körpers. Die Ideale zerfallen nun nach §. 153 in eine endliche Anzahl von Classen

$$A_1, A_2, \ldots, A_h,$$

und das grosse Ziel ist die Bestimmung dieser Zahl h, der Classenzahl.

Die Ideale $\mathfrak{a}_1$ einer dieser Classen A_1 sind dadurch charakterisirt, dass ihre Producte mit einem und demselben ganzen Functionale φ_1, das der Classe A_1^{-1} angehört, Hauptideale sind, dass also

$$\varphi_1\mathfrak{a}_1 = \alpha$$

eine ganze Zahl des Körpers Ω ist.

Ist die Norm von $\mathfrak{a}_1$ nicht grösser als t, so ist

$$N_a(\alpha) \mathrel{\substack{<\\=}} N_a(\varphi_1)\,t = t_1.$$

Ist T_1 die Anzahl der Ideale der Classe A_1, deren Normen nicht grösser als t sind, so ist T_1 zugleich die Anzahl der nicht

[1]) Die hier gebrauchten Sätze über Γ-Functionen finden sich in den ausführlicheren Lehrbüchern der Integralrechnung, z. B. Serret-Harnack, Lehrbuch der Differential- und Integralrechnung, Bd. II, S. 170 f. (Leipzig 1885).

associirten durch φ_1 theilbaren ganzen Zahlen, deren Normen nicht grösser als t_1 sind, und nach dem Satze §. 190, 1. ist

$$\text{(2)} \qquad \lim_{t_1 = \infty} \frac{T_1}{t_1} = \frac{g}{N_a(\varphi_1)},$$

wenn g die an der erwähnten Stelle angegebene Bedeutung hat, also eine von Null verschiedene, durch die Natur des Körpers Ω bestimmte Zahl ist.

Wenn jetzt $T_2, t_2, \ldots, T_h, t_h$ die entsprechende Bedeutung für die Classen $A_2, \ldots, A_h$ haben, wie T_1, t_1 für A_1, so ist

$$T = T_1 + T_2 + \cdots + T_h,$$

$$\frac{T}{t} = \frac{T_1}{t_1} N_a(\varphi_1) + \frac{T_2}{t_2} N_a(\varphi_2) + \cdots + \frac{T_h}{t_h} N_a(\varphi_h),$$

und aus (1) und (2) ergiebt sich die fundamentale Formel:

$$\text{(3)} \qquad \lim_{s=1} \sum \frac{s-1}{N(\mathfrak{a})^s} = g\,h.$$

Die Zahl g können wir nach §. 185, (11) als bekannt betrachten, wenn auch ihre wirkliche Berechnung noch auf der Voraussetzung beruht, dass ein Fundamentalsystem von Einheiten bekannt sei, und wenn auch die Ermittelung eines solchen Systemes in höheren Körpern immer als eine der grössten Schwierigkeiten betrachtet worden ist. Dann hängt die Berechnung der Classenzahl noch von der Bestimmung des Grenzwerthes auf der linken Seite von (3) ab, die natürlich auch nur in besonderen Fällen gelingt, doch aber oft wichtige Schlüsse über die Natur der Classenzahl gestattet. Wir wollen noch eine die Berechnung vorbereitende Umformung der Summe

$$\text{(4)} \qquad \sum \frac{1}{N(\mathfrak{a})^s} = \Phi(s)$$

in ein unendliches Product entwickeln.

Es sei $\mathfrak{p}$ irgend ein Primideal f^{ten} Grades im Körper Ω, also

$$N(\mathfrak{p}) = p^f.$$

Dann ist die unendliche geometrische Reihe

$$1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \cdots = \frac{1}{1 - p^{-sf}};$$

wenn man diese Reihen für alle verschiedenen Primideale $\mathfrak{p}$ mit einander multiplicirt, so erhält man nach bekannten Sätzen aus

der Lehre von den unendlichen Reihen eine Summe von Gliedern der Form

$$\left(\frac{1}{N(\mathfrak{p})^k}\,\frac{1}{N(\mathfrak{p}')^{k'}}\,\frac{1}{N(\mathfrak{p}'')^{k''}}\cdots\right)^s = \left(\frac{1}{N(\mathfrak{p}^k\mathfrak{p}'^{k'}\mathfrak{p}''^{k''}\ldots)}\right)^s,$$

die alle in der Form $N(\mathfrak{a})^{-s}$ enthalten sind, und jedes solche Glied ergiebt sich ein- und nur einmal. Danach ist also

$$(5) \qquad \Phi(s) = \Pi \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

Sind daher $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_e$ die von einander verschiedenen Primfactoren von p, und $f_1, f_2, \ldots, f_e$ ihre Grade (§. 143), so ergiebt sich

$$(6) \qquad \Phi(s) = \overset{p}{\Pi} \frac{1}{(1 - p^{-sf_1})(1 - p^{-sf_2})\ldots(1 - p^{-sf_e})},$$

worin das unendliche Product Π über alle natürlichen Primzahlen p auszudehnen ist, und nach (3), (4)

$$(7) \qquad gh = \operatorname*{Lim}_{s=1}\,(s-1)\,\Phi(s).$$

Hieraus lässt sich ein für mannigfache Anwendungen wichtiger Schluss ziehen:

Wenn wir aus der Entwickelung

$$1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots = \frac{1}{1 - p^{-s}}$$

das Product für alle Primzahlen p bilden, so ergiebt sich:

$$(8) \qquad \overset{p}{\Pi} \frac{1}{1 - p^{-s}} = \overset{n}{\Sigma} \frac{1}{n^s},$$

worin sich die Summe auf der rechten Seite auf alle natürlichen Zahlen n erstreckt, und es hat also dies Product für alle Werthe von s, die grösser als 1 sind, einen endlichen Werth. Der reciproke Werth, nämlich das Product

$$(9) \qquad P = \overset{p}{\Pi}\,(1 - p^{-s}),$$

dessen Factoren sämmtlich kleiner als 1 sind, hat daher, so lange $s > 1$ ist, einen von Null verschiedenen Werth. Diese Eigenschaft bleibt nun erhalten, wenn wir bei der Bildung des Productes P nur einen Theil aller Primzahlen p berücksichtigen, weil das Product durch Weglassen beliebiger Factoren nur vergrössert wird, ohne die Einheit je zu übersteigen.

Daraus ergiebt sich, dass in dem Producte (6) die Theilproducte

$$\Pi \frac{1}{1 - p^{-sf}},$$

die sich über alle Primzahlen p erstrecken, für die $f > 1$ ist, auch für $s = 1$ noch endlich bleiben. Da andererseits g, h bestimmte von Null verschiedene Werthe haben, so ergiebt sich aus (7) der wichtige Satz:

I. Durchläuft $\mathfrak{p}$ die Gesammtheit der Primideale ersten Grades irgend eines algebraischen Körpers Ω, so hat das Product

(10) $$(s - 1) \Pi \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

für $s = 1$ einen endlichen von Null verschiedenen Grenzwerth.

Diese Eigenschaft bleibt auch dann noch erhalten, wenn bei der Bildung des Productes eine beliebige endliche Anzahl von Primidealen ersten Grades ausgelassen wird.

Die Normen $N(\mathfrak{p})$ sind in der Formel (10) gleich natürlichen Primzahlen p. Eine Primzahl p kommt aber darin so oft vor, als sie Primfactoren ersten Grades in Ω enthält, also höchstens n mal. Ist Ω ein Normalkörper, so kommt auch wirklich jede Primzahl p, die in Primfactoren ersten Grades zerlegbar ist, genau n mal darin vor, und wir können für das Product (10) auch setzen:

$$(s - 1) \Pi \frac{1}{(1 - p^{-s})^n},$$

worin sich das Product Π auf alle in Primfactoren ersten Grades zerlegbaren Primzahlen p erstreckt (§. 160).

Eine unmittelbare Folgerung des Satzes I. ist die:

In jedem algebraischen Körper giebt es unendlich viele Primideale ersten Grades.

Vierundzwanzigster Abschnitt.

Classenzahl der Kreistheilungskörper.

§. 193.

Classenzahldarstellung im Kreistheilungskörper Ω_m.

Die allgemeinen Resultate über die Classenzahl h sollen nun angewandt werden auf den vollen Kreistheilungskörper Ω_m unter der bisherigen Voraussetzung, dass m eine Potenz einer Primzahl q sei, und dass also

(1) $$m = q^{\varkappa}, \quad \varphi(m) = q^{\varkappa-1}(q-1) = \mu$$

gesetzt sei.

Im einundzwanzigsten Abschnitte (§. 169, 171) haben wir gesehen, dass in q nur ein Primideal 1[sten] Grades aufgeht, und dass eine zum Exponenten f gehörige, von q verschiedene Primzahl p in e verschiedene Primideale f[ten] Grades zerfällt. Darin bedeutet f den kleinsten positiven Exponenten, für den

(2) $$p^f \equiv 1 \pmod{m}$$

ist, und e ist durch die Gleichung

(3) $$\mu = ef$$

bestimmt.

Die am Ende des vorigen Paragraphen durch die Formel (6) bestimmte Function $\Phi(s)$ erhält daher hier den Ausdruck:

(4) $$\Phi(s) = \frac{1}{1-q^{-s}} \Pi \frac{1}{(1-p^{-sf})^e},$$

und darin erstreckt sich das Productzeichen Π auf alle Primzahlen p, die von q verschieden sind. Darin ist s eine Variable, die immer grösser als 1 ist, die sich schliesslich der Grenze 1 nähern soll.

Um nun diesen Ausdruck für die Function Φ weiter umzuformen und zur Berechnung vorzubereiten, hat man die Sätze über die Abel'schen Gruppen und Gruppencharaktere zu benutzen, die wir in den Paragraphen 14 bis 16 dieses Bandes kennen gelernt haben.

Die Gesammtheit der durch q nicht theilbaren Zahlen n bildet, nach dem Modul m genommen, eine Abel'sche Gruppe $\mathfrak{N}$ vom Grade μ, deren Charaktere $\chi(n)$ im §. 16 bestimmt sind. Es war dabei ein kleiner Unterschied, je nachdem q ungerade oder $q = 2$ ist.

1) Ist q ungerade, so giebt es eine primitive Wurzel c von m, und für jede Zahl n giebt es einen Index γ, so dass

(5) $$n \equiv c^\gamma \pmod{m}.$$

Ist dann Θ eine μ^{te} Einheitswurzel, so ist

(6) $$\chi(n) = \Theta^\gamma,$$

und die sämmtlichen μ Charaktere erhält man, wenn man für Θ die verschiedenen μ^{ten} Einheitswurzeln setzt.

Gehört n zum Exponenten f, so ist e der grösste gemeinschaftliche Theiler von γ und μ, und $\chi(n)$ ist f^{te} Einheitswurzel.

2) Für $q = 2$, $m > 4$ (den Fall $m = 4$ berücksichtigen wir hier nicht) hat jede ungerade Zahl n zwei Indices α, β, die nach den Moduln 2, $\frac{1}{2}\mu$ bestimmt sind, für die

(7) $$n \equiv (-1)^\alpha 5^\beta \pmod{m}$$

ist. Als Charaktere erhält man, wenn $\varepsilon = \pm 1$ und Θ gleich einer $\frac{1}{2}\mu^{\text{ten}}$ Einheitswurzel gesetzt wird:

(8) $$\chi(n) = \varepsilon^\alpha \Theta^\beta;$$

f ist die kleinste positive Lösung der beiden Congruenzen:

$$\alpha f \equiv 0 \pmod{2}, \quad \beta f \equiv 0 \pmod{\tfrac{1}{2}\mu},$$

und $\chi(n)$ ist auch hier f^{te} Einheitswurzel.

Für beide Fälle gilt aber die Bemerkung:

3) Gehört n zum Exponenten f, so erhält man, wenn man χ die gesammte Gruppe der μ Charaktere durchlaufen lässt, aus $\chi(n)$ jede f^{te} Einheitswurzel e mal.

Denn da die χ eine Abel'sche Gruppe bilden, so erhält man zunächst jede f^{te} Einheitswurzel, die überhaupt vorkommt, gleich oft, nämlich so oft als den Werth 1, weil, wenn $\chi_1(n) = \chi_2(n)$ ist, $\chi_1 \chi_2^{-1}(n) = \chi_0(n) = 1$ ist. Andererseits erhält man aber

jede f^{te} Einheitswurzel; denn wenn man im Falle 1) für Θ eine primitive μ^{te}, im Falle 2) eine primitive $\frac{1}{2}\mu^{te}$ Einheitswurzel, und im letzten Falle zugleich $\varepsilon = -1$ setzt, so ist $\chi(n)$ eine primitive f^{te} Einheitswurzel und aus deren Potenzen kann man alle f^{ten} Einheitswurzeln herleiten.

Bedeutet daher jetzt x eine Variable, so ist, wenn n zum Exponenten f gehört, das über sämmtliche Charaktere χ erstreckte Product

$$(9) \qquad \prod^{\chi} [1 - \chi(n) x] = (1 - x^f)^e,$$

und wenn man daher $x = p^{-s}$ setzt, so ergiebt sich aus (4):

$$(10) \qquad \Phi(s) = \frac{1}{1 - q^{-s}} \prod^{\chi} \prod^{p} \frac{1}{1 - \chi(p) p^{-s}},$$

wenn sich das erste Productzeichen auf alle Charaktere χ, das zweite auf alle Primzahlen p erstreckt. Es ist also $\Phi(s)$ ein Product aus einer endlichen Zahl, μ, von Factoren, deren jeder ein unendliches Product ist.

Jetzt wollen wir jeden Factor eines dieser unendlichen Producte nach steigenden Potenzen von p^{-s} entwickeln. Dadurch ergiebt sich

$$\frac{1}{1 - \chi(p) p^{-s}} = 1 + \chi(p) p^{-s} + \chi(p^2) p^{-2s} + \chi(p^3) p^{-3s} + \cdots$$

Das Product aus allen Factoren, die man hieraus erhält, wenn χ festgehalten wird, während p alle von q verschiedenen Primzahlen durchläuft, ist ein Aggregat von Gliedern der Form

$$\chi(p^k) \chi(p'^{k'}) \chi(p''^{k''}) \cdots p^{-sk} p'^{-sk'} p''^{-sk''} \cdots = \chi(n) n^{-s},$$

und jedes Glied dieser Form kommt in dem Producte ein- und nur einmal vor [vgl. §. 192, (8)]. Danach ergiebt sich die Umformung von $\Phi(s)$ in ein endliches Product von unendlichen Reihen:

$$(11) \qquad \Phi(s) = \frac{1}{1 - q^{-s}} \prod^{\chi} \sum^{n} \frac{\chi(n)}{n^s},$$

worin sich die Summe auf alle durch q nicht theilbaren Zahlen n erstreckt und das Product auf alle μ Charaktere χ.

Dieser Ausdruck ist geeignet, um den Grenzwerth von $(s - 1)\Phi(s)$ für $s = 1$ zu bestimmen.

Betrachten wir zunächst die dem Hauptcharakter $\chi = 1$ entsprechende Summe

$$\sum^{n} \frac{1}{n^s}.$$

Man erhält die Zahlen n, wenn man von der Gesammtheit aller natürlichen Zahlen k die Vielfachen von q, d. h. die Gesammtheit der Zahlen qk wegnimmt. Hiernach ist

$$\Sigma \frac{1}{n^s} = \Sigma \frac{1}{k^s} - \Sigma \frac{1}{q^s k^s} = (1 - q^{-s}) \Sigma \frac{1}{k^s}.$$

Wenn man aber in dem Satze 3., §. 191, für die μ_n die Reihe der natürlichen Zahlen k setzt, so folgt:

$$\operatorname*{Lim}_{s=1} (s-1) \Sigma \frac{1}{k^s} = 1,$$

und wir erhalten daher

(12) $$\operatorname*{Lim}_{s=1} \frac{s-1}{1-q^{-s}} \Sigma \frac{1}{n^s} = 1.$$

Die anderen Factoren des Productes $\Phi(s)$ aber sind, wenn die unendlichen Reihen nach steigenden Werthen von n geordnet werden, nach dem Satze 1., §. 191, stetige Functionen von s.

Denn die nach steigenden Werthen von n geordnete Summe

(13) $$\Sigma \chi(n)$$

ist zwar nicht convergent, kann aber doch dem absoluten Werthe nach nicht über eine endliche Grenze hinausgehen. Denn so oft n ein volles Restsystem nach dem Modul m durchläuft, kommt zu der Summe (13) ein Beitrag hinzu, der nach §. 11, 6. den Werth 0 hat. Demnach ist, wenn χ nicht der Hauptcharakter ist,

(14) $$\operatorname*{Lim}_{s=1} \sum^{n} \frac{\chi(n)}{n^s} = \sum^{n} \frac{\chi(n)}{n},$$

und demnach erhalten wir für die Classenzahl h im Kreistheilungskörper Ω_m jetzt den Ausdruck

(15) $$gh = \prod^{\chi} \sum^{n} \frac{\chi(n)}{n},$$

in dem sich das Productzeichen Π nur noch auf die vom Hauptcharakter verschiedenen Charaktere χ bezieht.

§. 194.

Bestimmung der Summen X.

Die unendlichen Reihen

(1) $$X = \sum^{n} \frac{\chi(n)}{n},$$

von denen hiernach die Bestimmung der Classenzahl noch abhängt, lassen sich durch endliche Ausdrücke darstellen. Es ist nämlich

$$\frac{1}{n} = \int_0^1 x^{n-1}\, dx,$$

und demnach

$$X = \int_0^1 \Sigma\, \chi(n)\, x^{n-1}\, dx.$$

Nun bleibt $\chi(n)$ ungeändert, wenn n um ein Vielfaches von m wächst. Versteht man aber unter t den kleinsten positiven Rest von n und setzt

$$n = t + ml,$$

so ist $\chi(n) = \chi(t)$, und es folgt:

$$X = \int_0^1 \sum^t \chi(t)\, x^{t-1} \sum_{0,\infty}^l x^{ml}\, dx.$$

Setzt man jetzt

(2) $$f(x) = \sum^t \chi(t)\, x^t,$$

so ist $f(x)$ eine ganze Function von x vom Grade $m - 1$, und zugleich ist wegen der Relation $\Sigma\, \chi(t) = 0$:

(3) $$f(0) = 0, \quad f(1) = 0,$$

also $f(x)$ durch $x\,(1 - x)$ theilbar. Für X ergiebt sich dann nach der Summenformel für die geometrische Reihe $\Sigma\, x^{ml}$:

(4) $$X = \int_0^1 \frac{f(x)\, dx}{x\,(1 - x^m)}.$$

Um ein solches Integral zu finden, schreibt die Integralrechnung vor, den rationalen Bruch unter dem Integralzeichen in Partialbrüche zu zerlegen. Diese Partialbruch-Zerlegung ergiebt aber, wegen (3), wenn

$$r = e^{\frac{2\pi i}{m}}$$

gesetzt wird:

$$\frac{f(x)}{x\,(1 - x^m)} = -\frac{1}{m} \sum_{1,\, m-1}^{s} \frac{f(r^s)}{x - r^s}$$

[Bd. I, §. 29, (11)], und nun haben wir weiter nach bekannten

elementaren Sätzen der Integralrechnung, wenn α irgend einen Winkel zwischen 0 und 2π bedeutet,

$$\int_0^1 \frac{dx}{x - e^{i\alpha}} = \tfrac{1}{2} \log \left(4 \sin^2 \frac{\alpha}{2}\right) + i \, \frac{\pi - \alpha}{2}.$$

Hieraus ergiebt sich nach (4):

$$(5) \quad X = -\frac{1}{m} \sum_{1, m-1}^{s} f(r^s) \left[\tfrac{1}{2} \log 4 \left(\sin \frac{s\pi}{m}\right)^2 - \frac{i\pi (m - 2s)}{2m}\right].$$

Hierin ist nach (2)

$$(6) \qquad f(r^s) = \sum^{t} \chi(t)\, r^{ts},$$

und daraus ergiebt sich [wegen (3)]:

$$(7) \qquad \sum_{1, m-1}^{s} f(r^s) = \sum_{0, m-1}^{s} f(r^s) = 0,$$

da

$$\sum_{0, m-1}^{s} r^{st} = 0$$

ist. Hiernach vereinfacht sich die Formel (5) noch etwas und ergiebt

$$(8) \qquad X = -\frac{1}{m} \sum_{1, m-1}^{s} f(r^s) \left[\tfrac{1}{2} \log \left(\sin \frac{s\pi}{m}\right)^2 + \frac{i\pi s}{m}\right],$$

wofür man auch, wenn man s durch $m - s$ ersetzt und wieder (7) benutzt,

$$(9) \qquad X = -\frac{1}{m} \sum_{1, m-1}^{s} f(r^{-s}) \left[\tfrac{1}{2} \log \left(\sin \frac{s\pi}{m}\right)^2 - \frac{i\pi s}{m}\right]$$

setzen kann.

Aus (6) folgt aber

$$f(r^{-s}) = \sum^{t} \chi(t)\, r^{-ts},$$

und die nach t genommene Summe ändert sich nicht, wenn t durch $m - t$ ersetzt wird. Daraus folgt:

$$f(r^{-s}) = \chi(-1)\, f(r^s).$$

Der Factor $\chi(-1)$ hat den Werth $+1$ oder -1, da sein Quadrat $= +1$ ist. Wir unterscheiden daher jetzt zwei Arten von Charakteren $\chi_1(n)$, $\chi_2(n)$, so dass

$$(10) \qquad \chi_1(-1) = 1, \quad \chi_2(-1) = -1$$

ist, und danach sind auch die Functionen f in f_1 und f_2 zu unterscheiden, so dass

(11) $$f_1(r^{-s}) = f_1(r^s),\quad f_2(r^{-s}) = -f_2(r^s)$$

wird. Ebenso unterscheiden wir die Ausdrücke (8), (9) als X_1 und X_2, und es ergiebt sich, wenn man beide Ausdrücke addirt, nach (11):

(12) $$X_1 = -\frac{1}{2m}\sum_{1,m-1}^{s} f_1(r^s)\log\left(\sin\frac{s\pi}{m}\right)^2,$$
$$X_2 = -\frac{i\pi}{m^2}\sum_{1,m-1}^{s} s f_2(r^s).$$

§. 195.

Ueber die Classenzahl in dem in Ω_m enthaltenen reellen Körper.

Unsere allgemeinen Principien können auch angewandt werden, um die Classenzahlen in den Theilern des Körpers Ω_m zu bestimmen.

Insbesondere sind die Formeln (6), (7), §. 192 anwendbar, wenn wir die Grade der Primideale in einem solchen Theiler kennen. Die Frage nach dem Verhältniss der Classenzahlen in den Theilern eines Körpers Ω_m zu der Classenzahl in Ω_m selbst ist von grossem Interesse und soll hier für den Fall behandelt werden, dass es sich um den in Ω_m enthaltenen reellen Körper H_m handelt, den wir ja schon im §. 176 f. untersucht haben [1]). Es hat sich dort ergeben, dass q im Körper H_m die $\frac{1}{2}\mu^{\text{te}}$ Potenz einer Primzahl ersten Grades ist, dass die anderen Primzahlen p in e_1 Primfactoren f_1^{ten} Grades zerfallen, so dass

(1) $$f_1 e_1 = \tfrac{1}{2}\mu,$$

und dass zwei Arten von Primzahlen p_1, p_2 zu unterscheiden sind, so dass bei den Primzahlen erster Art $f_1 = \frac{1}{2}f$, $e_1 = e$, bei denen der zweiten Art $f_1 = f$, $e_1 = \frac{1}{2}e$ ist.

Für den Körper H_m erhalten wir demnach aus §. 192, (6), (7) die Classenzahl h_1 nach der Formel:

[1]) Vgl. Kummer, „Bestimmung der Anzahl u. s. f.". Crelle's Journ., Bd. 40 (1849).

(2) $$g_1 h_1 = \lim_{s=1} (s-1)\, \Phi_1(s),$$

(3) $$\Phi_1(s) = \frac{1}{1-q^{-s}} \prod^{p_1} \frac{1}{(1-p_1^{-\frac{1}{2}sf})^e} \prod^{p_2} \frac{1}{(1-p_2^{-sf})^{\frac{1}{2}e}},$$

worin sich die beiden Productzeichen auf alle Primzahlen p_1 und p_2 beziehen. Mit Benutzung der oben erklärten Zeichen f_1, e_1 kann man dafür auch setzen:

(4) $$\Phi_1(s) = \frac{1}{1-q^{-s}} \prod^{p} \frac{1}{(1-p^{-sf_1})^{e_1}},$$

und das Productzeichen auf alle Primzahlen p erstrecken.

Die Bedeutung von g_1 ergiebt sich aus §. 190, (11).

Nun wollen wir aus der Gruppe C der Charaktere χ einen Theiler C_1 aussondern, der aus allen den Charakteren χ_1 bestehen soll, für die

(5) $$\chi_1(-1) = +1$$

ist. Zunächst ist klar, dass diese Charaktere χ_1 eine Gruppe C_1 bilden. Diese Gruppe ist aber nicht mit C identisch, weil es gewiss einen Charakter χ_0 giebt, für den $\chi_0(-1) = -1$ ist. Wir brauchen, um einen solchen zu erhalten, nur in §. 193, (6) für Θ eine primitive μ^{te} Einheitswurzel, oder in §. 193, (8) $\varepsilon = -1$ zu setzen. Dann bildet die Gesammtheit der Charaktere $\chi_0 \chi_1$, die alle nicht zu C_1 gehören, eine Nebengruppe C_2, deren Elemente mit χ_2 bezeichnet werden mögen. Jeder Charakter χ ist also dann entweder in C_1 oder in C_2 enthalten, denn wenn χ nicht in C_1 vorkommt, so kommt $\chi_0^{-1}\chi$ darin vor, und folglich χ in C_2. Es ist daher C_1 ein Theiler von C vom Index 2.

Die Charaktere χ_1 kann man auf folgende Art bilden:

1) Ist m ungerade, so setzen wir, wie in §. 193,

$$n \equiv c^\gamma \pmod{m},$$

und lassen in

(6) $$\chi_1(n) = \Theta^\gamma$$

Θ die Gesammtheit der $\frac{1}{2}\mu^{\text{ten}}$ Einheitswurzeln durchlaufen.

2) Ist m gerade, so setzen wir

$$n \equiv (-1)^\alpha\, 5^\beta,$$

und erhalten

(7) $$\chi_1(n) = \Theta^\beta,$$

worin Θ wieder die sämmtlichen $\frac{1}{2}\mu^{\text{ten}}$ Einheitswurzeln durchläuft.

Beides ergiebt sich leicht dadurch, dass für $n = -1$ im ersten Falle $\gamma = \frac{1}{2}\mu$, im zweiten $\alpha = 1$, $\beta = 0$ ist, also beide Male $\chi_1(-1) = 1$ ist, und dass jede der Formeln (6), (7) genau $\frac{1}{2}\mu$ verschiedene Charaktere darstellt.

Worauf es nun wesentlich ankommt, ist Folgendes:

> Ist p irgend eine von q verschiedene Primzahl, so erhält man in der Form $\chi_1(p)$, wenn χ_1 die Gruppe C_1 durchläuft, jede f_1^{te} Einheitswurzel, und jede gleich oft, also e_1 mal.

Dass alle $\chi_1(p)$ Einheitswurzeln vom Grade f_1 sind, ist klar, denn es ist immer (vgl. §. 177) $p^{f_1} \equiv \pm 1 \pmod{m}$, und daher

$$[\chi_1(p)]^{f_1} = \chi_1(\pm 1) = 1.$$

Wenn aber unter den $\chi_1(p)$ eine primitive f_1^{te} Einheitswurzel vorkommt, so kommen alle anderen f_1^{ten} Einheitswurzeln auch darunter vor, und gleich oft, nämlich so oft wie die Einheitswurzel 1.

Dies folgt unmittelbar aus der Gruppennatur der χ_1. Es ist also nun noch zu zeigen, dass unter den $\chi_1(p)$ eine primitive f_1^{te} Einheitswurzel vorkommt.

Diese Möglichkeit ergiebt sich aber aus der Bestimmung von χ_1 sehr einfach. Ist zunächst Θ in (6) bei ungeradem m eine primitive Einheitswurzel vom Grade $\frac{1}{2}\mu$, und ist γ der Index von p, so ist eine Potenz von Θ^γ, $\Theta^{\gamma\lambda}$ dann und nur dann $= 1$, wenn

$$2\gamma\lambda \equiv 0 \pmod{\mu}.$$

Nun ist $\mu = ef$ und e der grösste gemeinschaftliche Theiler von γ und μ; und daher wird diese Bedingung $2\lambda \equiv 0 \pmod{f}$. Es ist aber nach §. 177, 3. $f_1 = f$ oder $= \frac{1}{2}f$, je nachdem f ungerade oder gerade ist, und folglich muss $\lambda \equiv 0 \pmod{f_1}$ sein. Also ist Θ^γ primitive f_1^{te} Einheitswurzel.

Ist aber m gerade, so nehmen wir in (7) gleichfalls für Θ eine primitive $\frac{1}{2}\mu^{\text{te}}$ Einheitswurzel und setzen

$$p \equiv (-1)^\alpha 5^\beta \pmod{m},$$

so dass f die kleinste positive Zahl ist, die den Congruenzen

$$\alpha f \equiv 0 \pmod{2}, \quad \beta f \equiv 0 \pmod{\tfrac{1}{2}\mu}$$

genügt. Es ist nun $\Theta^{\beta\lambda}$ nur dann $= 1$, wenn $\beta\lambda \equiv 0 \pmod{\frac{1}{2}\mu}$ ist. Wenn nicht $\lambda = 1$, also $\beta = 0$ ist, so ist der kleinste Werth, den λ haben kann, gerade, und daher ist dieser kleinste Werth von $\lambda = f$.

Wenn aber $\lambda = 1$ ist, so muss $\beta = 0$ sein, und es sind noch zwei Fälle möglich:

entweder $f = 1,\ \alpha = 0,\ p \equiv 1 \pmod{m},\ \lambda = f$
oder $f = 2,\ \alpha = 1,\ p \equiv -1 \pmod{m},\ \lambda = \frac{1}{2}f.$

Nur in diesem letzten Falle gehört p zur ersten Art, und es folgt also, dass auch hier allgemein Θ^{β} eine primitive f_1^{te} Einheitswurzel ist. Hiermit ist dann der Satz bewiesen.

Dieser Satz gestattet uns die Anwendung der Formel §. 193, (9), die hier ergiebt:

(8) $$(1 - p^{-sf_1})^{e_1} = \prod^{\chi_1} [1 - \chi_1(p) p^{-s}],$$

worin sich das Product auf alle Charaktere χ_1 der Gruppe C_1 erstreckt, und nun lässt sich die Function $\Phi_1(s)$ ebenso wie $\Phi(s)$ im §. 193 weiter entwickeln. Man erhält auf demselben Wege, wie dort, die Formel (11),

(9) $$\Phi_1(s) = \frac{1}{1 - q^{-s}} \prod^{\chi_1} \sum^{n} \frac{\chi_1(n)}{n^s},$$

und wenn man zur Grenze $s = 1$ übergeht,

(10) $$g_1 h_1 = \prod^{\chi_1} \sum^{n} \frac{\chi_1(n)}{n},$$

worin aber jetzt das Product auf alle Charaktere der Gruppe C_1 mit Ausnahme des Hauptcharakters zu erstrecken ist. Dieses Product ist also ein Theil des Productes, durch welches im §. 193 die Zahl gh ausgedrückt ist.

Die Zahlen g, g_1 ergeben sich aus dem im §. 190, (11) angegebenen allgemeinen Ausdrucke:

(11) $$\frac{2^{\nu} \pi^{n-\nu} L}{w \sqrt{\pm \Delta}}.$$

Da, wie im §. 178 nachgewiesen ist, die Einheiten in Ω_m und H_m, von den Einheitswurzeln abgesehen, dieselben sind, so ist auch ein Fundamentalsystem von Einheiten in H_m zugleich ein Fundamentalsystem in Ω_m.

Bedeutet $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ daher ein Fundamentalsystem reeller Einheiten, und sind $\varepsilon_{i,1}, \varepsilon_{i,2}, \ldots, \varepsilon_{i,\nu}$ die conjugirten Einheiten zu ε_i, so sind die conjugirten Logarithmen im Körper H_m:

$$\log|\varepsilon_{i,1}|,\ \log|\varepsilon_{i,2}|,\ \ldots,\ \log|\varepsilon_{i,\nu}|,$$

dagegen im Körper Ω_m, in dem nur conjugirt imaginäre Paare vorkommen (§. 185),

$$2\log|\varepsilon_{i,1}|,\ 2\log|\varepsilon_{i,2}|,\ \ldots,\ 2\log|\varepsilon_{i,\nu}|.$$

Bezeichnen wir daher mit

$$(12) \quad E = \pm \begin{vmatrix} \log|\varepsilon_{1,1}|, & \log|\varepsilon_{1,2}|, & \ldots, & \log|\varepsilon_{1,\nu-1}| \\ \log|\varepsilon_{2,1}|, & \log|\varepsilon_{2,2}|, & \ldots, & \log|\varepsilon_{2,\nu-1}| \\ \cdot & \cdot & \cdot & \cdot \\ \log|\varepsilon_{\nu-1,1}|, & \log|\varepsilon_{\nu-1,2}|, & \ldots, & \log|\varepsilon_{\nu-1,\nu-1}| \end{vmatrix}$$

den Regulator des Körpers H_m (§. 187), so ist bei der Anwendung des Ausdruckes (11) im Körper Ω_m

$$L = 2^{\nu-1} E,$$

und im Körper H_m

$$L = E$$

zu setzen. Es ist ferner

$$\text{in } \Omega_m: \quad n = \mu, \quad \nu = \tfrac{1}{2}\mu,$$
$$\text{in } H_m: \quad n = \tfrac{1}{2}\mu, \quad \nu = \tfrac{1}{2}\mu.$$

Im Körper H_m sind nur die zwei Einheitswurzeln ± 1 enthalten. In Ω_m sind die mit positivem und negativem Zeichen genommenen Potenzen von r, sonst aber keine Einheitswurzeln enthalten (§. 175), und bei der Zählung ist noch zu beachten, dass bei geradem m unter den Potenzen von r auch -1 enthalten ist, bei ungeradem m nicht. Daher haben wir

$$\text{in } \Omega_m: \quad w = 2m, \quad m \text{ ungerade}$$
$$= m, \quad m \text{ gerade},$$
$$\text{in } H_m: \quad w = 2.$$

Endlich haben wir noch, wenn Δ, Δ_1 die Grundzahlen der Körper Ω_m, H_m sind (§. 176):

$$\pm \Delta = q \Delta_1^2 \quad m \text{ ungerade}$$
$$= 4 \Delta_1^2 \quad m \text{ gerade},$$

und es folgt, wenn wir der Einfachheit wegen ν für $\frac{1}{2}\mu$ setzen:

$$g = \frac{2^{2(\nu-1)} \pi^\nu E}{m \sqrt{q}\, \Delta_1} \quad m \text{ ungerade}$$

$$g = \frac{2^{2(\nu-1)} \pi^\nu E}{m \Delta_1} \quad m \text{ gerade},$$

$$(13) \quad g_1 = \frac{2^{\nu-1} E}{\sqrt{\Delta_1}},$$

woraus

$$(14) \quad \begin{aligned} g &= \frac{2^{\nu-1} \pi^\nu g_1}{m \sqrt{q \Delta_1}} \quad m \text{ ungerade} \\ g &= \frac{2^{\nu-1} \pi^\nu g_1}{m \sqrt{\Delta_1}} \quad m \text{ gerade.} \end{aligned}$$

Wenn wir die Formel (10) mit der Formel §. 193, (15) verbinden und die im §. 194 eingeführte Bezeichnung

$$X_1 = \sum^n \frac{\chi_1(n)}{n}, \quad X_2 = \sum^n \frac{\chi_2(n)}{n}$$

gebrauchen, so ergiebt sich

$$g\,h = g_1 h_1 \,\Pi\, X_2.$$

Ersetzt man g durch seinen Werth (14), so folgt für die Classenzahl

(15) $$h = k\,h_1,$$

wenn

(16) $$k = \frac{m\sqrt{q\,\Delta_1}}{2^{\nu-1}\,\pi^\nu}\,\Pi\,X_2 \quad \text{bei ungeradem } m$$

$$= \frac{m\sqrt{\Delta_1}}{2^{\nu-1}\,\pi^\nu}\,\Pi\,X_2 \quad \text{bei geradem } m,$$

und worin [nach (10), (13)]:

(17) $$h_1 = \frac{\sqrt{\Delta_1}}{2^{\nu-1}\,E}\,\Pi\,X_1$$

die Classenzahl des Körpers H_m ist. Im letzteren Ausdrucke erstreckt sich das Product auf alle Charaktere χ_1 der Gruppe C_1 mit Ausnahme des Hauptcharakters.

Dass k eine ganze Zahl ist, und daher h ein Vielfaches von h_1, wird sich bald zeigen. Die Zahlen k und h_1 heissen der erste und zweite Factor der Classenzahl.

In dem Falle, dass

$$m = 2^\varkappa$$

eine Potenz von 2 ist, haben wir nach §. 176, (7):

$$\Delta_1 = 2^{(\varkappa-1)2^{\varkappa-2}-1},$$

und wenn wir diesen Werth einsetzen, so können wir für die vorstehenden Formeln in diesem Falle schreiben:

(18) $$k = \frac{\sqrt{2}\;2^{2^{\varkappa-3}(\varkappa-3)}\,2^\varkappa}{\pi^\nu}\,\Pi\,X_2$$

$$h_1 = \frac{\sqrt{2}\;2^{2^{\varkappa-3}(\varkappa-3)}}{E}\,\Pi\,X_1.$$

§. 196.

Classenzahl im Körper der achten Einheitswurzeln.

Wir wollen, einerseits zur Veranschaulichung der bisherigen Resultate, andererseits um für die später anzuwendende vollständige Induction eine Basis zu gewinnen, den Fall $m = 8$, $\mu = 4$, $\nu = 2$ zunächst behandeln.

Hier haben wir ausser dem Hauptcharakter nur drei Charaktere, nämlich, wenn

$$n \equiv (-1)^\alpha 5^\beta \pmod 8)$$

ist,

$$\chi_1(n) = (-1)^\beta$$
$$\chi_2(n) = (-1)^\alpha$$
$$\chi_3(n) = (-1)^{\alpha+\beta}.$$

Für $n = -1$ ist $\alpha = 1$, $\beta = 0$, und folglich gehört χ_1 zur ersten, χ_2, χ_3 zur zweiten Art [§. 195, (5)], und es ergeben sich für die vier Zahlen $n = 1, 3, 5, 7$ folgende Werthe dieser Charaktere:

$$\begin{array}{lrrrr} \chi_1: & +1, & -1, & -1, & +1 \\ \chi_2: & +1, & -1, & +1, & -1 \\ \chi_3: & +1, & +1, & -1, & -1. \end{array}$$

Daraus erhält man die drei Functionen f_1, f_2, f_3 [§. 194, (2)]:

$$f_1(x) = x - x^3 - x^5 + x^7 = x(1-x^2)(1-x^4)$$
$$f_2(x) = x - x^3 + x^5 - x^7 = x(1-x^2)(1+x^4)$$
$$f_3(x) = x + x^3 - x^5 - x^7 = x(1+x^2)(1-x^4).$$

Für r können wir setzen:

$$r = \frac{1+i}{\sqrt{2}}, \quad r^2 = i, \quad r^3 = -\frac{1-i}{\sqrt{2}}, \quad r^4 = -1,$$

und danach ergiebt sich:

$$\begin{array}{lll} f_1(r) = 2\sqrt{2}, & f_2(r) = 0, & f_3(r) = 2\sqrt{2}\, i, \\ f_1(r^2) = 0, & f_2(r^2) = 4i, & f_3(r^2) = 0, \\ f_1(r^3) = -2\sqrt{2}, & f_2(r^3) = 0, & f_3(r^3) = 2\sqrt{2}\, i. \end{array}$$

Für $x = r^4$ verschwinden alle drei Functionen $f(x)$, und für $x = r^5, r^6, r^7$ erhält $f_1(x)$ dieselben, $f_2(x)$ und $f_3(x)$ die entgegengesetzten Werthe, wie für $x = r^3, r^2, r$.

Demnach ergiebt sich aus §. 194, (12) mit Rücksicht auf die trigonometrische Formel

$$\sin\frac{3\pi}{8} = \cos\frac{\pi}{8}$$

$$X_1 = -\frac{1}{\sqrt{2}}\log \operatorname{tg}\frac{\pi}{8},\quad X_2 = \frac{-\pi}{4},\quad X_3 = \frac{-\pi}{2\sqrt{2}}.$$

Nun ist

$$\tau = \frac{r-1}{r^2(r+1)} = \operatorname{tg}\frac{\pi}{8} = \sqrt{2} - 1$$

eine Einheit des Körpers H_8, der hier nichts Anderes ist, als der aus $\sqrt{2}$ entspringende quadratische Körper, und die Einheiten darin erhält man also aus den Lösungen der Pell'schen Gleichung

$$u^2 - 2v^2 = \pm 1$$

in der Form $u + v\sqrt{2}$.

Die kleinste positive Lösung dieser Pell'schen Gleichung ist aber $u = 1$, $v = 1$, und folglich findet man nach Bd. I, §. 128 alle Einheiten in H_8 in der Form $\pm(1+\sqrt{2})^a$, worin a ein positiver oder negativer ganzzahliger Exponent ist; τ ergiebt sich hieraus für $a = -1$, und daher sind alle Einheiten auch in der Form

$$\pm\,\tau^a$$

enthalten. Es ist also τ eine fundamentale Einheit, und die in den Formeln des vorigen Paragraphen vorkommende Determinante E [§. 195, (12)] wird hier (da τ ein echter Bruch ist):

$$E = -\log\tau.$$

Man erhält also aus §. 195, (15), (18):

$$h_1 = 1,\quad k = 1,\quad h = 1.$$

Der Körper Ω_8 ist also ein einclassiger, d. h. ein solcher, in dem die Zerlegung der ganzen Zahlen in Primfactoren nach denselben Gesetzen, wie im Körper der rationalen Zahlen, möglich ist.

Es hat sich dabei zugleich ergeben, dass alle Einheiten im Körper H_8 in der Form $\pm\,\tau^a$ darstellbar sind. Die conjugirten Werthe der Einheit τ sind aber

$$\tau_1 = \operatorname{tg}\frac{\pi}{8},\quad \tau_3 = -\operatorname{tg}\frac{3\pi}{8} = -\tau_1^{-1},$$

und haben also verschiedene Zeichen. Wir schliessen daraus für diesen Fall auf den Satz:

Eine Einheit in H_3, die mit ihren Conjugirten von einerlei Zeichen ist, ist, vom Zeichen abgesehen, das Quadrat einer Einheit.

§. 197.

Recurrente Berechnung der Classenzahl im Körper Ω_m, wenn m eine Potenz von 2 ist.

Zur allgemeinen Bestimmung der Classenzahl im Körper Ω_m unter der Voraussetzung, dass m irgend eine Potenz von 2 und grösser als 8 ist, wenden wir ein recurrirendes Verfahren an. Es sei also

(1) $$m = 2^\varkappa, \quad \mu = 2^{\varkappa-1}, \quad \nu = 2^{\varkappa-2}, \quad \nu' = 2^{\varkappa-3}.$$

Neben dem Körper Ω_m betrachten wir den Körper Ω_μ, der ein Theiler von Ω_m ist, und den wir hier auch mit Ω'_m bezeichnen wollen. Es sei h' die Classenzahl im Körper Ω'_m, d. h. die Zahl, die sich aus h ergiebt, wenn $\varkappa$ in $\varkappa - 1$ verwandelt wird, und wir setzen

(2) $$h = h' H.$$

Setzen wir h' als schon bekannt voraus, so kommt es nur noch auf die Berechnung von H an, was, wie sich zeigen wird, eine ganze Zahl ist. Indem wir h und h' wie im §. 195 zerlegen, setzen wir

(3) $$h = k h_1, \quad h' = k' h'_1,$$
(4) $$k = k' A, \quad h_1 = h'_1 B, \qquad H = A B,$$

worin k' aus k und h'_1 aus h_1 durch die Vertauschung von $\varkappa$ mit $\varkappa - 1$ hervorgeht. Wir wollen überhaupt jetzt durch Accente an den Buchstaben andeuten, dass $\varkappa - 1$ statt $\varkappa$ gesetzt sein soll.

Nach §. 176, (7) ist dann

$$\Delta_1 = 2^{(\varkappa-1)2^{\varkappa-2}-1},$$
$$\Delta'_1 = 2^{(\varkappa-2)2^{\varkappa-3}-1},$$

und folglich

(5) $$\Delta_1 = 2^{\varkappa 2^{\varkappa-3}} \Delta'_1.$$

Hat E die Bedeutung §. 195, (12), und geht E' aus E hervor, wenn $\varkappa$ durch $\varkappa - 1$ ersetzt wird, so setzen wir noch

(6) $$E = E' D,$$

wodurch D als eine von Null verschiedene positive Zahl definirt ist. Was die Summen

$$X = \Sigma \frac{\chi(n)}{n}$$

betrifft, so ist daran zu erinnern, dass $\chi(n)$ [nach §. 193, (8)] definirt ist durch

$$(7) \qquad n \equiv (-1)^\alpha\, 5^\beta \pmod{m}, \quad \chi(n) = (\pm 1)^\alpha\, \Theta^\beta,$$

worin Θ eine ν^{te} Einheitswurzel bedeutet.

Unter den ν^{ten} Einheitswurzeln sind aber auch die ν'^{ten} Einheitswurzeln enthalten, und unter den Charakteren χ auch die Charaktere für den Körper Ω'_m. Wir unterscheiden demnach primitive und imprimitive Charaktere des Körpers Ω_m, indem wir die dem Körper Ω_m eigenthümlichen Charaktere χ, d. h. die, in denen Θ eine primitive ν^{te} Einheitswurzel ist, als primitiv bezeichnen.

Unter den Summen X kommen auch alle zu dem Körper Ω'_m gehörigen Summen vor:

$$X' = \Sigma \frac{\chi'(n)}{n}.$$

Wenn man nun in (4) für k, k' und h_1, h'_1 die im §. 195, (16), (17) gebildeten Ausdrücke einsetzt, und dann die Summen X' weghebt, so ergiebt sich:

$$(8) \qquad \begin{aligned} \pi^{\nu'} A &= 2 . 2^{2^{\varkappa-4}(\varkappa-2)} \prod X_2 \\ D B &= 2^{2^{\varkappa-4}(\varkappa-2)} \prod X_1, \end{aligned}$$

worin sich jetzt aber die Producte $\prod$ nur noch auf die mit den primitiven Charakteren χ_1, χ_2 gebildeten Summen X_1, X_2 erstrecken.

In den im §. 194, (12) gegebenen Ausdrücken für die X:

$$(9) \qquad \begin{aligned} X_1 &= -\frac{1}{2m} \sum_{1, m-1}^{s} f_1(r^s) \log \left(\sin \frac{s\pi}{m}\right)^2 \\ X_2 &= -\frac{i\pi}{m^2} \sum_{1, m-1}^{s} s f_2(r^s) \end{aligned}$$

treten nun, unter der Voraussetzung, dass m eine Potenz von 2 und dass χ_1, χ_2 primitive Charaktere sind, bedeutende Vereinfachungen ein.

Die Zahl $1 + \mu$ hat die Indices $\alpha = 0$, $\beta = \nu'$, und folglich ist nach (7)

$$\chi(1 + \mu) = \Theta^{\nu'} = -1,$$

wenn χ ein primitiver Charakter ist.

Ferner ist für ein ungerades n:

$$n(1 + \mu) \equiv n + \mu \pmod{m},$$

und folglich

$$\chi(n + \mu) = -\chi(n).$$

Wenn wir nun die Function $f(r^s)$ betrachten:

$$(10) \qquad f(r^s) = \sum^{n} \chi(n)\, r^{sn},$$

worin n die ungeraden Zahlen eines vollen Restsystems für den Modul m durchläuft, so erhalten wir, da wir in (10) unter dem Summenzeichen n durch $n + \mu$ ersetzen dürfen:

$$f(r^s) = -r^{\mu s} \sum \chi(n)\, r^{sn},$$

und da $r^{\mu} = -1$ ist:

$$f(r^s) = -(-1)^s f(r^s).$$

Es ist also

(11) $\qquad f(r^s) = 0$, wenn s gerade ist,

und demnach können wir in den Formeln (9) den Summationsbuchstaben s auf die ungeraden Zahlen beschränken, die kleiner als m sind.

Es ist aber nach (10):

$$f(r^s) = \chi(s)^{-1} \sum^{n} \chi(ns)\, r^{sn},$$

und wenn man sn durch n ersetzt, was bei ungeradem s gestattet ist:

(12) $\qquad f(r^s) = \chi(s)^{-1} f(r)$, wenn s ungerade ist.

Die Function $f(r)$ hat, wenn α, β die Indices von n sind, den Ausdruck

$$(13) \qquad f(r) = \sum^{n} (\pm 1)^{\alpha}\, \Theta^{\beta} r^{n},$$

und ist also mit der im §. 17 dieses Bandes betrachteten Kreistheilungsresolvente

$$(\pm 1, \Theta, r)$$

gleichbedeutend, für die im §. 17, (17) die Relation aufgestellt war:

$$(14) \qquad (\pm 1, \Theta, r)(\pm 1, \Theta^{-1}, r) = \pm m.$$

Hier gelten durchweg die oberen Zeichen für die Summen X_1, die unteren für die Summen X_2 [§. 195, (7)].

Wir theilen jetzt die Reihe der in (9) vorkommenden Zahlen s in vier Theile. Es soll t ein Zeichen sein, welches die

Reihe der positiven ungeraden Zahlen von 1 bis $\nu - 1$ durchläuft; dann durchläuft das ungerade s die vier Zahlenreihen:

$$t,\ t+\mu,\ m-t,\ m-t-\mu,$$

und es ist:

$$\chi(t+\mu) = -\chi(t),$$
$$\chi_1(m-t) = \chi_1(t),\quad \chi_1(m-\mu-t) = -\chi_1(t),$$
$$\chi_2(m-t) = -\chi_2(t),\quad \chi_2(m-\mu-t) = \chi_2(t).$$

Nach (12) ergiebt sich hieraus:

$$f(r^{t+\mu}) = -f(r^t),$$
$$f_1(r^{m-t}) = f_1(r^t),\quad f_1(r^{m-\mu-t}) = -f_1(r^t),$$
$$f_2(r^{m-t}) = -f_2(r^t),\quad f_2(r^{m-\mu-t}) = f_2(r^t).$$

Theilt man demnach die Summen (9) in je vier Theile und benutzt noch die trigonometrische Gleichung

$$\sin\frac{(t+\mu)\pi}{m} = \cos\frac{t\pi}{m},$$

so ergiebt sich

$$X_1 = \frac{-1}{m}\sum^t f_1(r^t)\log\left(\operatorname{tg}\frac{t\pi}{m}\right)^2,$$

$$X_2 = \frac{i\pi}{m}\sum^t f_2(r^t).$$

In dieser Summe ist

$$\frac{t\pi}{m} < \frac{\pi}{4},\quad \operatorname{tg}\frac{t\pi}{m} > 0,$$

und folglich erhalten wir mit Rücksicht auf (12), (13), wenn wir Θ^{-1} für Θ setzen, wodurch $\chi(t)^{-1}$ in $\chi(t)$ übergeht:

$$(15)\qquad X_1 = -\frac{2}{m}(+1, \Theta^{-1}, r)\sum^t \chi_1(t)\log\left(\operatorname{tg}\frac{t\pi}{m}\right),$$

$$(16)\qquad X_2 = \frac{i\pi}{m}(-1, \Theta^{-1}, r)\sum^t \chi_2(t),$$
$$1 \leqq t \leqq \nu - 1.$$

§. 198.

Der Classenzahlfactor A.

Um nun zunächst A zu berechnen, haben wir den Ausdruck (16) für X_2 in die erste Formel (8) des vorigen Paragraphen einzusetzen. Diese Formel können wir auch so darstellen:

$$(1)\qquad \pi^{\nu'} A = 2 m^{1/4\nu}\, 2^{-\nu'} \prod X_2.$$

Bezeichnen wir mit α, β die Indices von t, so ist $\chi_2(t) = (-1)^\alpha \Theta^\beta$;

$$(2) \qquad \sum^{t} \chi_2(t) = \Sigma (-1)^\alpha \Theta^\beta = \varphi(\Theta)$$

ist eine ganze Zahl des Körpers Ω_ν, und es wird:

$$X_2 = \frac{i\pi}{m}(-1, \Theta^{-1}, r)\, \varphi(\Theta).$$

Nun hat man für Θ alle Wurzeln der Gleichung

$$(3) \qquad \Theta^{\nu'} + 1 = 0$$

zu setzen, und erhält für A, mit Rücksicht auf §. 197, (14):

$$(4) \qquad A = 2^{1-\nu'} \prod^{\Theta} \varphi(\Theta).$$

Die Summe, durch die in (2) die Zahl $\varphi(\Theta)$ definirt ist, enthält ν' Glieder von der Form $(-1)^\alpha \Theta^\beta$, worin α, β so zu bestimmen sind, dass

$$(5) \qquad (-1)^\alpha 5^\beta \equiv t \pmod{m}$$

und t zwischen 0 und ν liegt. Nun ist zunächst ersichtlich, dass unter den Exponenten β nicht zwei nach dem Modul ν' congruente vorkommen können. Denn ist $\beta \equiv \beta' \pmod{\nu'}$, so ist $5^\beta \equiv 5^{\beta'} \pmod{\mu}$, und aus

$$(-1)^\alpha 5^\beta \equiv t, \quad (-1)^{\alpha'} 5^{\beta'} \equiv t' \pmod{m}$$

folgt:

$$(-1)^\alpha t - (-1)^{\alpha'} t' \equiv 0 \pmod{\mu}.$$

Da aber t und t' absolut kleiner als $\nu = \frac{1}{2}\mu$ sind, so ist dies nur möglich, wenn $t = t'$, $\alpha = \alpha'$ ist. Demnach durchläuft β in (2) ein volles Restsystem nach dem Modul ν'.

Da aber β nach dem Modul ν zu nehmen ist, so werden die nach (5) bestimmten β theils kleiner, theils grösser als ν' ausfallen, und wenn wir also β_1 die Reihe der Zahlen $0, 1, \ldots, \nu' - 1$ durchlaufen lassen, so erhalten wir in (2) zweierlei Arten von Gliedern:

$$(6) \qquad \begin{aligned} &1. \quad (-1)^\alpha \Theta^\beta = (-1)^\alpha \Theta^{\beta_1}, & \beta = \beta_1 < \nu', \\ &2. \quad (-1)^\nu \Theta^\beta = -(-1)^\alpha \Theta^{\beta_1}, & \beta = \beta_1 + \nu' \geqq \nu'. \end{aligned}$$

Nun ist nach (5) der absolut kleinste Rest von $(-1)^\alpha 5^\beta$ nach dem Modul m positiv, und wenn wir daher eine Zahl $c_\beta = \pm 1$ so bestimmen, dass der absolut kleinste Rest von $c_\beta 5^\beta$ positiv wird, so ist in dem Falle (6), 1.

$$c_{\beta_1} = (-1)^\alpha.$$

Ferner ist $5^{\nu'} \equiv 1 \pmod{\mu}$, und da $5^{\nu'}$ nicht auch nach dem Modul m mit 1 congruent ist, so folgt:

(7) $$5^{\nu'} \equiv 1 + \mu \pmod{m}.$$

Demnach ist im Falle (6), 2.

$$(-1)^\alpha 5^\beta = (-1)^\alpha 5^{\beta_1} 5^{\nu'} \equiv (-1)^\alpha 5^{\beta_1} + \mu \pmod{m},$$

und folglich ist hier der absolut kleinste Rest von $(-1)^\alpha 5^{\beta_1}$ nach dem Modul m negativ. Es ist also im Falle (6), 2.

$$c_{\beta_1} = -(-1)^\alpha$$

zu setzen.

Daraus ergiebt sich nach (2) (wenn wir wieder β für β_1 schreiben):

(8) $$\varphi(\Theta) = \sum_{0,\nu'-1}^{\beta} c_\beta \Theta^\beta$$
$$= c_0 + c_1 \Theta + c_2 \Theta^2 + \cdots + c_{\nu'-1} \Theta^{\nu'-1},$$

und hierin ist

(9) $$c_\beta = +1 \quad \text{oder} \quad = -1,$$

je nachdem der absolut kleinste Rest von 5^β positiv oder negativ ist. Hiernach ist also $\varphi(\Theta)$ eine ganze Zahl des Körpers Ω_ν.

Es kommt noch darauf an, das Verhalten dieser Zahl zu der Zahl 2, oder vielmehr zu dem in Ω_ν enthaltenen Primfactor $(1 - \Theta)$ von 2 zu ermitteln. Bilden wir zu diesem Zwecke

(10) $$(1 - \Theta)\, \varphi(\Theta) = 2\, \psi(\Theta),$$

so ergiebt sich

(11) $$\psi(\Theta) = \frac{c_0 + c_{\nu'-1}}{2} + \frac{c_1 - c_0}{2} \Theta + \frac{c_2 - c_1}{2} \Theta^2 + \cdots$$
$$+ \frac{c_{\nu'-1} - c_{\nu'-2}}{2} \Theta^{\nu'-1}.$$

Die Coëfficienten in diesem Ausdrucke sind alle $= 0$ oder $= 1$, und daher ist auch $\psi(\Theta)$ eine ganze Zahl des Körpers Ω_ν. Für diese Zahl ergiebt sich aber, wenn man $\Theta \equiv 1$ setzt:

(12) $$\psi(\Theta) \equiv c_{\nu'-1} \equiv \pm 1 \; [\mathrm{mod}\, (1 - \Theta)],$$

und folglich ist $\psi(\Theta)$ relativ prim zu 2.

Das in (4) vorkommende Product ist nichts Anderes, als die in Bezug auf den Körper Ω_ν genommene Norm der Zahl $\varphi(\Theta)$, und wenn wir diese Norm mit N bezeichnen, so ist nach §. 169

$$N(1 - \Theta) = 2,$$

und folglich nach (10)

$$N\varphi(\Theta) = 2^{\nu'-1} N\psi(\Theta).$$

Daraus ergiebt sich

(13) $$A = N\psi(\Theta),$$

und hieraus folgt mit Rücksicht auf (12), dass A eine ungerade ganze Zahl ist.

Bezeichnen wir die zu $m = 2^{\varkappa}$ gehörige Zahl A mit $A_{\varkappa}$, so ergiebt sich aus §. 197, (4) durch vollständige Induction der Ausdruck für den ersten Factor der Classenzahl:

(14) $$k = A_4 A_5 \dots A_{\varkappa},$$

und daraus der Satz:

1. Der erste Factor der Classenzahl ist eine ungerade ganze Zahl.

Die Zahl $A_{\varkappa}$ ist nach der Formel (10) für die ersten Werthe von $\varkappa$ nicht schwer zu berechnen.

Für $m = 16$ findet man $\nu' = 2$, $\beta = 0, 1$, $c_0 = c_1 = 1$ folglich

$$\psi(\Theta) = 1, \quad A_4 = 1.$$

Für $m = 32$, $\nu' = 4$, $\beta = 0, 1, 2, 3$.

$$c_0 = 1, \; c_1 = 1, \; c_2 = -1, \; c_3 = -1,$$
$$\psi(\Theta) = -\Theta^2,$$

also auch $A_5 = 1$.

Für $m = 64$, $\nu' = 8$, $\beta = 0, 1, 2, 3, 4, 5, 6, 7$ sind die absolut kleinsten Reste von 5^{β}

$$1, 5, 25, -3, -15, -11, 9, -19;$$

also sind die c_{β}:

$$+1, +1, +1, -1, -1, -1, +1, -1$$

und

$$\psi(\Theta) = -\Theta^3 + \Theta^6 - \Theta^7, \quad \psi(\Theta)\psi(-\Theta) = \Theta^6(\Theta^6 - 2i),$$

woraus sich leicht ergiebt:

$$A_6 = 17.$$

Eine etwas längere Rechnung ergiebt noch

$$A_7 = 21121.$$

§. 199.

Der Classenzahlfactor B.

Auf ganz andere Weise muss der Classenzahlfactor B berechnet werden. Hier ist, wenn Θ wieder eine Primitivwurzel der Gleichung §. 198, (3) ist ($\Theta^{\nu'} + 1 = 0$), und

(1) $$t \equiv (-1)^{\alpha}\, 5^{\beta} \pmod{m},$$

(2) $$\chi_1(t) = \Theta^{\beta}$$

zu setzen, und die Formel §. 197, (15) ergiebt:

(3) $$X_1 = -\frac{2}{m}(1, \Theta^{-1}, r) \sum^{t} \Theta^{\beta} \log \operatorname{tg} \frac{t\pi}{m}.$$

Nun ist für jedes ungerade t, wenn [mit Rücksicht auf (1)]

$$r = e^{\frac{2\pi i}{m}},\ r^{\nu} = i,\ r^{\nu t} = (-1)^{\alpha} i$$

gesetzt wird,

(4) $$\operatorname{tg} \frac{t\pi}{m} = (-1)^{\alpha}\, r^{t\nu}\, \frac{1 - r^{t}}{1 + r^{t}},$$

und dies ist, wie wir schon im §. 178 gesehen haben, eine Einheit des reellen Körpers H_m. Man erhält die conjugirten Werthe dieser Einheit in Bezug auf diesen Körper, wenn man $t \equiv 5^{\beta}$ (mod m) setzt, und β ein volles Restsystem nach dem Modul μ durchlaufen lässt. Wir setzen demnach:

(5) $$\tau_{\beta} = \operatorname{tg} \frac{5^{\beta}\pi}{m}.$$

Nach §. 198, (7) ist $5^{\beta+\nu'} \equiv 5^{\beta} + \mu \pmod{m}$, und daraus ergiebt sich nach einer bekannten trigonometrischen Formel:

(6) $$\tau_{\beta+\nu'} = \frac{-1}{\tau_{\beta}}.$$

Setzen wir also nun

(7) $$\lambda_{\beta} = \tfrac{1}{2} \log \tau_{\beta}^{2},$$

so ist nach (6)

(8) $$\lambda_{\beta+\nu'} = -\lambda_{\beta},$$

und demnach

(9) $$\Theta^{\beta+\nu'} \lambda_{\beta+\nu'} = \Theta^{\beta} \lambda_{\beta};$$

unter den in der Summe (3) vorkommenden Werthen von β sind, wie wir schon im vorigen Paragraphen gesehen haben, nicht zwei nach dem Modul ν' congruent, und wenn wir daher mittelst

der Formel (9) alle Werthe von β auf das Intervall von 0 bis $\nu' - 1$ reduciren, so bekommen wir alle Zahlen dieses Intervalles.

Demnach lässt sich die Formel (3) so darstellen:

$$X_1 = -\frac{2}{m}(1, \Theta^{-1}, r) \sum_{0, \nu'-1}^{\beta} \Theta^\beta \lambda_\beta. \tag{10}$$

Dies haben wir in dem im §. 197, (8) angegebenen Ausdrucke

$$DB = 2^{2^{\varkappa-4}(\varkappa-2)} \prod X_1 = m^{\nu''} 2^{-\nu'} \prod X_1$$

einzusetzen, und dann ergiebt sich, wenn wir

$$U_\Theta = \sum_{0, \nu'-1}^{\beta} \Theta^\beta \lambda_\beta \tag{11}$$

setzen, mit Rücksicht auf §. 197, (14):

$$DB = \prod^{\Theta} U_\Theta. \tag{12}$$

Dies Product lässt sich nun auf folgende Weise durch eine Determinante darstellen, die nur die conjugirten Logarithmen der Einheiten τ enthält.

Lassen wir den Index Θ bei U weg, so können wir das Gleichungssystem ansetzen:

$$\begin{array}{ll} U & = \lambda_0 + \lambda_1 \Theta + \lambda_2 \Theta^2 + \cdots + \lambda_{\nu'-1} \Theta^{\nu'-1} \\ \Theta U & = -\lambda_{\nu'-1} + \lambda_0 \Theta + \lambda_1 \Theta^2 + \cdots + \lambda_{\nu'-2} \Theta^{\nu'-1} \\ \cdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \Theta^{\nu'-1} U & = -\lambda_1 - \lambda_2 \Theta - \lambda_3 \Theta^2 + \cdots + \lambda_0 \Theta^{\nu'-1}, \end{array}$$

woraus durch Elimination der Potenzen von Θ folgt:

$$\begin{vmatrix} \lambda_0 - U, & \lambda_1, & \lambda_2, \ldots, \lambda_{\nu'-1} \\ -\lambda_{\nu'-1}, & \lambda_0 - U, & \lambda_1, \ldots, \lambda_{\nu'-2} \\ \cdots & \cdots & \cdots \\ -\lambda_1, -\lambda_2, & -\lambda_3, & \ldots, \lambda_0 - U \end{vmatrix} = 0. \tag{13}$$

Dies ist für U eine Gleichung ν'^{ten} Grades, deren Wurzeln die Grössen U_Θ sind. Ordnet man nach Potenzen von U, so erhält, da ν' gerade ist, die höchste Potenz $U^{\nu'}$ von U den Coëfficienten 1, und man findet also das in (12) vorkommende Product der Wurzeln, wenn man $U = 0$ setzt, aus der Determinante (13).

Die so gewonnene Determinante wollen wir etwas anders anordnen, indem wir die erste Zeile an ihrer Stelle lassen, die

übrigen aber in umgekehrter Ordnung und mit verändertem Vorzeichen schreiben. Dabei sind $\frac{1}{2}\nu'$ Vorzeichenänderungen nöthig, und wir erhalten daher für das Product (12) die durch folgende Gleichung definirte Determinante, deren absoluten Werth wir mit T bezeichnen:

$$(14) \qquad (-1)^{\frac{1}{2}\nu'} \begin{vmatrix} \lambda_0, & \lambda_1, \ldots, & \lambda_{\nu'-2}, & \lambda_{\nu'-1} \\ \lambda_1, & \lambda_2, \ldots, & \lambda_{\nu'-1}, & -\lambda_0 \\ \lambda_2, & \lambda_3, \ldots, & -\lambda_0, & -\lambda_1 \\ \cdot & \cdot & \cdot & \cdot \\ \lambda_{\nu'-1}, & -\lambda_0, \ldots, & -\lambda_{\nu'-3}, & -\lambda_{\nu'-2} \end{vmatrix} = \pm T,$$

worin rechts von der von links unten nach rechts oben laufenden Diagonalreihe die negativen Zeichen stehen.

Die Determinante T ist hier so geordnet, dass jede Zeile aus der vorangehenden durch die Substitution $(r, r^{5^{\beta}})$ entsteht. Jede Colonne enthält also ein System conjugirter Logarithmen.

Nach (12) ist jetzt

$$(15) \qquad B = \frac{T}{D}.$$

Um über die Natur dieses Resultates Klarheit zu bekommen, ist es nöthig, die Zahl D etwas genauer zu betrachten, die durch §. 195, (12), §. 197, (6) definirt war; und dies erfordert ein Eingehen auf die Theorie der Einheiten des Körpers H_m.

§. 200.

Normaleinheiten in H_m.

Wir führen jetzt eine vereinfachende Bezeichnung ein, indem wir

$$(1) \qquad r^{5^{\beta}} = r_{\beta}$$

setzen, und β ein volles Restsystem nach dem Modul ν durchlaufen lassen. Es folgt hieraus

$$(2) \qquad r_{\beta+\nu'} = -r_{\beta},$$

und in der Form (r, r_{β}) sind dann zwar nicht alle Substitutionen der Gruppe des Körpers Ω_m enthalten, sondern es müssen noch die Substitutionen (r, r_{β}^{-1}) hinzukommen; wohl aber liefert uns (r, r_{β}) alle Substitutionen der Gruppe von H_m.

Wir bezeichnen jetzt mit $\mathfrak{E}(r)$ eine Einheit des Körpers H_m. Unter diesen sind auch die Einheiten des Körpers H_{μ} (als

imprimitive Zahlen) enthalten und durch die Gleichung $\mathfrak{E}(r) = \mathfrak{E}(-r)$ charakterisirt.

Wir wollen nun unter einer **Normaleinheit** des Körpers H_m eine Einheit verstehen, die nicht $= \pm 1$ ist, aber der Gleichung

(3) $$\mathfrak{E}(r)\, \mathfrak{E}(-r) = \pm 1$$

genügt.

Es ist klar, dass eine Einheit des Körpers H_μ dieser Bedingung jedenfalls nicht genügen kann. Aber nicht jede Einheit in H_m, die dem Körper H_μ nicht angehört, wird Normaleinheit sein [1]).

Die Einheiten τ_β [§. 199, (5)] gehören aber zu den Normaleinheiten. Es ist nämlich

(4) $$\tau_\beta = \operatorname{tg} \frac{5^\beta \pi}{m} = \frac{1 - r_\beta}{1 + r_\beta}\, r_\beta^\nu,$$

und wenn darin die Substitution $(r, -r) = (r_\beta, r_{\beta+\nu'})$ gemacht wird, so geht τ_β in

(5) $$\tau'_{\beta+\nu'} = -\frac{1}{\tau_\beta}$$

über, was der Relation (3) entspricht.

Ein System von ν' Normaleinheiten

$$\mathfrak{E}_0(r),\, \mathfrak{E}_1(r), \ldots, \mathfrak{E}_{\nu'-1}(r)$$

soll ein **unabhängiges System** heissen, wenn die Determinante

(6) $$\pm \Sigma \pm \log |\mathfrak{E}_0(r_0)| \log |\mathfrak{E}_1(r_1)| \ldots \log |\mathfrak{E}_{\nu'-1}(r_{\nu'-1})| = L(\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\nu'-1})$$

einen von Null verschiedenen Werth hat.

Den absoluten Werth dieser Determinante, L, nennen wir auch hier den **Regulator** des Systems $\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\nu'-1}$.

Die Einheiten $\tau_0, \tau_1, \ldots, \tau_{\nu'-1}$ bilden ein unabhängiges System normaler Einheiten, denn ihr Regulator

$$L(\tau_0, \tau_1, \ldots, \tau_{\nu'-1})$$

ist eben die im vorigen Paragraphen definirte Determinante T [§. 199, (14), (15)]. Und dass diese nicht Null sein kann, ergiebt sich unmittelbar daraus, dass sie in dem Ausdrucke für die

---

[1]) Der Verfasser hat in der oben erwähnten Arbeit (Acta mathematica, Bd. 8) die Normaleinheiten als „primitive Einheiten" bezeichnet. Dieser Name ist hier verworfen, weil er zu dem Irrthum Veranlassung geben könnte, als ob jede Einheit des Körpers H_m, die nicht zugleich dem Körper H_μ angehört, dazu zu rechnen sei.

Classenzahl als Factor vorkommt. Die Classenzahl ist aber, da gewiss immer wenigstens eine Classe, die Hauptclasse, existirt, von Null verschieden, und also kann auch T nicht gleich Null sein. Wir haben daher den Satz:

1. Die Zahlen $\tau_0, \tau_1, \ldots, \tau_{\nu'-1}$ sind ein unabhängiges System von Normaleinheiten des Körpers H_m.

Ist $\mathfrak{E}(r)$ eine Normaleinheit, so ist, wenn wir

(7) $$L_\beta = \log |\mathfrak{E}(r_\beta)|$$

setzen, wegen (3)

(8) $$L_\beta = - L_{\beta+\nu'}.$$

Ist nun $\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\nu'-1}$ irgend ein System unabhängiger Normaleinheiten, so setzen wir:

(9) $$L_{i,k} = \log |\mathfrak{E}_i(r_k)|, \quad L_{i,k+\nu'} = - L_{i,k},$$

so dass der Regulator des Systems der $\mathfrak{E}_i$ den Ausdruck erhält:

(10) $$\pm \Sigma \pm L_{0,0} L_{1,1} \ldots L_{\nu'-1,\nu'-1} = L(\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\nu'-1}),$$

und eine von Null verschiedene Zahl ist, die wir mit T_0 bezeichnen.

Bedeutet $\mathfrak{E}(r)$ irgend eine andere Normaleinheit, so können wir die Unbekannten $\xi_0, \xi_1, \ldots, \xi_{\nu'-1}$ aus den ν' linearen Gleichungen bestimmen, die wir erhalten, wenn wir in

(11) $$L_\beta = \xi_0 L_{0,\beta} + \xi_1 L_{1,\beta} + \cdots + \xi_{\nu'-1} L_{\nu'-1,\beta}$$

den Index β von 0 bis $\nu' - 1$ gehen lassen, und wegen (8) und (9) ist diese Gleichung auch für die übrigen Werthe von β richtig, so dass man daraus die für alle r gültige Formel ableiten kann:

(12) $$\mathfrak{E}(r) = \pm \mathfrak{E}_0(r)^{\xi_0} \mathfrak{E}_1(r)^{\xi_1} \ldots \mathfrak{E}_{\nu'-1}(r)^{\xi_{\nu'-1}}.$$

Bedeuten andererseits $m_0, m_1, \ldots, m_{\nu'-1}$ irgend welche ganze rationale Zahlen, so sind alle in der Form

$$\pm \mathfrak{E}_0(r)^{m_0} \mathfrak{E}_1(r)^{m_1} \ldots \mathfrak{E}_{\nu'-1}(r)^{m_{\nu'-1}}$$

enthaltenen Zahlen Normaleinheiten des Körpers H_m. Demnach lassen sich auf das Gleichungssystem (10) die Betrachtungen anwenden, die wir im §. 186 ausführlich durchgeführt haben, woraus sich ergiebt:

2. Die aus (10) oder (11) bestimmten Exponenten $\xi_0, \xi_1, \ldots, \xi_{\nu'-1}$ sind rationale Zahlen.

Hieraus kann, wie im §. 187, gefolgert werden, dass es Systeme von ν' unabhängigen Normaleinheiten giebt, deren Regulator T_0 so klein als möglich wird, und solche Systeme heissen Fundamentalsysteme von Normaleinheiten.

Ist $\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\nu'-1}$ ein solches Fundamentalsystem, so ergeben sich die Exponenten $\xi_0, \xi_1, \ldots, \xi_{\nu'-1}$ in (10) und (11) als ganze rationale Zahlen. Auch dies kann ebenso bewiesen werden, wie im §. 187.

Stellen wir unter dieser Voraussetzung über die $\mathfrak{E}_i$ die Gleichungen (11) für irgend ein anderes System unabhängiger Einheiten $\mathfrak{E}_0^{(1)}, \mathfrak{E}_1^{(1)}, \ldots, \mathfrak{E}_{\nu'-1}^{(1)}$ auf, so erhalten wir Ausdrücke von der Form:

$$L_{i,k}^{(1)} = \xi_{i,0} L_{0,k} + \xi_{i,1} L_{1,k} + \cdots + \xi_{i,\nu'-1} L_{\nu'-1,k}.$$

Ist also T_1 der Regulator des Systems der $\mathfrak{E}_i^{(1)}$, so ergiebt sich nach dem Multiplicationssatze der Determinanten, wenn mit C der absolute Werth der Determinante der ganzzahligen Exponenten $\xi_{i,k}$, also eine ganze rationale positive Zahl bezeichnet wird:

(13) $$T_1 = C\, T_0.$$

Es kann nicht bewiesen werden und trifft für die höheren Werthe von m wahrscheinlich auch nicht zu, dass $\tau_0, \tau_1, \ldots, \tau_{\nu'-1}$ ein Fundamentalsystem bilden [1]).

Für unseren Zweck ist es aber von Wichtigkeit, dass sich diese Einheiten in Bezug auf den Nenner 2 in den Exponenten

---

[1]) Es ist hier, wie bei allen Fragen, die die Einheiten betreffen, sehr schwierig, zu bestimmten numerischen Resultaten zu gelangen. Nach den Resultaten, die in dem reichhaltigen Werke von Reuschle, „Tafeln complexer Primzahlen, welche aus Wurzeln der Einheiten gebildet sind" (Berlin 1875), enthalten sind, bilden für $m = 16$ die τ noch ein Fundamentalsystem. Denn hier ist die Grundzahl des Körpers H_m gleich 2^{11}, der Grad des Körpers gleich 4, und daher giebt es nach der Anmerkung zu §. 156 in jeder Idealclasse ein Ideal, dessen Norm kleiner als 6 ist. Nach den Tafeln von Reuschle kann aber jede natürliche Primzahl unter 100 im Körper H_m in wirklich existirende Primfactoren zerlegt werden. Folglich gehen gewiss in allen Zahlen unter 6 nur Hauptideale auf, und folglich giebt es hier nur die eine Classe, die Hauptclasse. Da, wie wir gesehen haben, auch der erste Classenzahlfactor $= 1$ ist, so ist der Kreistheilungskörper Ω_{16} einclassig. Es gelten in ihm dieselben Gesetze der Primzahlen, wie im Körper der rationalen Zahlen. Zweifelhaft ist dies für den Körper Ω_{32} und sicher nicht mehr zutreffend im Körper Ω_{64}, in dem die Classenzahl ein Vielfaches von 17 ist.

gewissermaassen wie ein Fundamentalsystem verhalten, was durch folgenden Satz bestimmter ausgedrückt wird:

2. Wenn eine Normaleinheit des Körpers H_m von der Form

$$\mathfrak{E}(r) = \tau_0^{e_0}\,\tau_1^{e_1}\,\ldots\,\tau_{\nu'-1}^{e_{\nu'-1}},$$

in der die Exponenten $e_0, e_1, \ldots, e_{\nu'-1}$ ganze rationale Zahlen sind, mit allen ihren conjugirten Werthen einerlei Vorzeichen hat, so müssen die sämmtlichen $e_0, e_1, \ldots, e_{\nu'-1}$ gerade Zahlen sein, und $\mathfrak{E}(r)$ ist das Quadrat einer Normaleinheit.

Den Beweis können wir wieder durch vollständige Induction führen, wollen aber zunächst den Ausdruck für τ_β etwas umformen.

Die conjugirten Werthe zu der Einheit $\mathfrak{E}(r)$ erhalten wir in der Form

$$\mathfrak{E}(r_\beta) = \tau_\beta^{e_0}\,\tau_{\beta+1}^{e_1}\,\ldots\,\tau_{\beta+\nu'-1}^{e_{\nu'-1}},$$

und diese Ausdrücke sollen also für alle Werthe von β dasselbe Vorzeichen haben.

Es ist nach §. 199, (5)

$$\tau_\beta = \operatorname{tg}\frac{5^\beta \pi}{m} = \frac{1}{2}\,\frac{\sin\left(\frac{2\pi}{m}\,5^\beta\right)}{\left[\cos\left(\frac{5^\beta\pi}{m}\right)\right]^2}.$$

Hierin setzen wir zur Abkürzung

$$(14)\qquad \sigma_\beta = \sin\left(\frac{2\pi}{m}\,5^\beta\right),$$

so dass σ_β immer dasselbe Vorzeichen hat, wie τ_β.

Daraus bilden wir das Product

$$(15)\qquad S_\beta = \sigma_\beta^{e_0}\,\sigma_{\beta+1}^{e_1}\,\ldots\,\sigma_{\beta+\nu'-1}^{e_{\nu'-1}},$$

und unsere Voraussetzung ist also die, dass S_β für alle Werthe von β dasselbe Vorzeichen hat.

Es soll nachgewiesen werden, dass die ganzen Zahlen $e_0, e_1, \ldots, e_{\nu'-1}$ alle gerade sein müssen.

Der Satz ist richtig für $m = 8$; denn in diesem Falle ist

$$\sigma_0 = \sin\frac{2\pi}{8},\quad \sigma_1 = \sin\frac{10\pi}{8} = -\sin\frac{6\pi}{8},$$

also σ_0 positiv, σ_1 negativ. Hier ist nun $S_\beta = \sigma_\beta^{e_0}$, und es kann also S_0 und S_1 nur dann gleiches Vorzeichen haben, wenn e_0 gerade ist.

Hiernach wenden wir die vollständige Induction an. Wir setzen zur Vereinfachung $\nu' = 2\nu''$ und erinnern an die Bezeichnung

$$(16) \qquad m = 2^\varkappa, \quad \mu = \tfrac{1}{2} m, \quad \nu = \tfrac{1}{2}\mu, \quad \nu' = \tfrac{1}{2}\nu, \quad \nu'' = \tfrac{1}{2}\nu',$$

und setzen voraus, dass unser Satz als richtig erwiesen sei, wenn μ an die Stelle von m tritt.

Es ist dann

$$5^\nu \equiv 1 \pmod{m}, \quad 5^{\nu'} \equiv 1 + \mu \pmod{m}, \quad 5^{\nu''} \equiv 1 + \nu \pmod{\mu}$$
$$5^{\nu''} \equiv 1 + \nu + \mu \pmod{m}$$

und daraus ergiebt sich

$$\sigma_{\beta+\nu'} = -\sigma_\beta,$$
$$\sigma_{\beta+\nu''} = -\cos\left(\frac{2\pi}{m} 5^\beta\right),$$
$$(17) \qquad \sigma_\beta\,\sigma_{\beta+\nu''} = -\tfrac{1}{2}\sin\left(\frac{2\pi}{\mu} 5^\beta\right) = -\tfrac{1}{2}\sigma'_\beta,$$
$$(18) \qquad \sigma'_{\beta+\nu''} = -\sigma'_\beta,$$

wenn die σ'_β aus den σ_β durch den Uebergang von $\varkappa$ zu $\varkappa - 1$ hervorgehen. Nun bilden wir nach (17), (18) das Product $S_\beta\, S_{\beta+\nu''}$, und erhalten, wenn noch zur Abkürzung

$$e' = e_0 + e_1 + \cdots + e_{\nu'-1}, \quad e'' = e_0 + e_1 + \cdots + e_{\nu''-1}$$

gesetzt wird,

$$S_\beta\, S_{\beta+\nu''} = (-1)^{e''} \left(\tfrac{1}{2}\right)^{e'} \sigma'^{\,e_0 + e_{\nu''}}_\beta\, \sigma'^{\,e_1 + e_{\nu''+1}}_{\beta+1} \cdots \sigma'^{\,e_{\nu''-1} + e_{\nu'-1}}_{\beta+\nu''-1}.$$

Dies ist aber ein Product von derselben Form wie S_β, in dem μ an Stelle von m getreten ist, was gleichfalls mit allen seinen Conjugirten einerlei Vorzeichen hat. Es ist daher nach der gemachten Voraussetzung

$$(19) \qquad e_0 \equiv e_{\nu''+1}, \; e_1 \equiv e_{\nu''+1}, \; \ldots, \; e_{\nu''-1} \equiv e_{\nu'-1} \pmod{2}.$$

Setzen wir also

$$S'_\beta = \sigma'^{\,e_0}_\beta\, \sigma'^{\,e_1}_{\beta+1} \cdots \sigma'^{\,e_{\nu''-1}}_{\beta+\nu''-1},$$
$$R_\beta = \sigma^{1/2(e_0 - e_{\nu''})}_{\beta+\nu''}\, \sigma^{1/2(e_1 - e_{\nu''+1})}_{\beta+\nu''+1} \cdots \sigma^{1/2(e_{\nu''-1} - e_{\nu'-1})}_{\beta+\nu'-1},$$

so folgt aus (15) und (17)

$$S_\beta\, R_\beta^2 = \left(-\tfrac{1}{2}\right)^{e''} S'_\beta,$$

und hieraus ergiebt sich, dass S'_β ebenso wie S_β mit allen seinen conjugirten Werthen dasselbe Zeichen hat. S'_β entsteht aber aus S_β dadurch, dass μ an Stelle von m gesetzt wird, und nach unserer Voraussetzung ist daher

$$e_0 \equiv 0,\ e_1 \equiv 0, \ldots, e_{\nu''-1} \equiv 0 \pmod 2,$$

und mit Hülfe von (19)

$$e_{\nu''} \equiv 0,\ e_{\nu''+1} \equiv 0, \ldots, e_{\nu'-1} \equiv 0 \pmod 2,$$

wodurch der Beweis des Satzes 2. geführt ist.

Wenn wir nun in der Formel (12) für $\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\nu'-1}$ das System $\tau_0, \tau_1, \ldots, \tau_{\nu'-1}$ wählen und die Exponenten ξ in die Form setzen:

$$\xi_0 = \frac{e_0}{e},\ \xi_1 = \frac{e_1}{e}, \ldots, \xi_{\nu'-1} = \frac{e_{\nu'-1}}{e},$$

worin $e, e_0, e_1, \ldots, e_{\nu'-1}$ ganze rationale Zahlen ohne gemeinsamen Theiler sind, so erhalten wir

$$\mathfrak{E}(r)^e = \pm\, \tau_0^{e_0}\, \tau_1^{e_1} \ldots \tau_{\nu'-1}^{e_{\nu'-1}},$$

und es folgt aus unserem Satze, dass e ungerade sein muss; denn wäre es gerade, so wäre $\mathfrak{E}(r)^e$ ein Quadrat einer reellen Grösse, und folglich hätte $\pm\, \mathfrak{E}(r)^e$ mit seinen Conjugirten dasselbe Vorzeichen. Dann aber müssten nach unserem Satze alle $e_0, e_1, \ldots, e_{\nu'-1}$ durch 2 theilbar sein, was wieder gegen die Voraussetzung ist, dass die Exponenten $e, e_0, \ldots, e_{\nu'-1}$ keinen gemeinsamen Theiler haben sollen. Wir haben daher den Satz:

3. Ist $\mathfrak{E}(r)$ irgend eine Normaleinheit des Körpers H_m, so lassen sich die ungerade Zahl e und die ganzen Zahlen $e_0, e_1, \ldots, e_{\nu'-1}$ so bestimmen, dass

(20) $$\mathfrak{E}(r_\beta)^e = \pm\, \tau_\beta^{e_0}\, \tau_{\beta+1}^{e_1} \ldots \tau_{\beta+\nu'-1}^{e_{\nu'-1}}$$

wird.

Dies Ergebniss führt zu einigen wichtigen Consequenzen:

4. Ist T der Regulator des Systems der τ_β, und T_0 der Regulator eines Fundamentalsystems normaler Einheiten in H_m, d. h. der Minimalwerth, den der Regulator irgend eines Systems unabhängiger Normaleinheiten annehmen kann, so ist

(21) $$T = C T_0, \quad C \equiv 1 \pmod 2,$$

worin C eine ungerade natürliche Zahl bedeutet.

Dass nämlich $T : T_0 = C$ eine ganze Zahl ist, folgt aus der Formel (13).

Wenn wir aber den Satz 3. auf alle Elemente des Fundamentalsystems $\mathfrak{E}_i(r)$ anwenden, so ergiebt sich ein System ganzer Zahlen $e_{i,k}$ und eine ungerade Zahl e, so dass

$$\mathfrak{E}_i(r)^e = \pm\, \tau_0^{e_{i,0}}\, \tau_1^{e_{i,1}} \ldots \tau_{\nu'-1}^{e_{i,\nu'-1}}.$$

Nehmen wir hiervon die Logarithmen, und bilden dann den Regulator T_0, so ergiebt sich

$$e^{\nu'} T_0 = \pm\, \Sigma \pm e_{0,0}\, e_{1,1} \ldots e_{\nu'-1,\nu'-1}\, T,$$

folglich

$$e^{\nu'} = \pm\, C\, \Sigma \pm e_{0,0}\, e_{1,1} \ldots e_{\nu'-1,\nu'-1},$$

und da hierin die linke Seite ungerade ist, so kann C nicht gerade sein, w. z. b. w.

Wenn alle conjugirten Werthe der Normaleinheit $\mathfrak{E}(r_\beta)$ einerlei Zeichen haben, so gilt dasselbe auch von $\mathfrak{E}(r_\beta)^e$, und folglich müssen in diesem Falle in der Formel (20) die Exponenten $e_0, e_1, \ldots, e_{\nu'-1}$ nach 2. gerade Zahlen sein. Schreibt man dann die Formel (20) so:

$$\mathfrak{E}(r) = \pm\, \tau_0^{e_0}\, \tau_1^{e_1} \ldots \tau_{\nu'-1}^{e_{\nu'-1}}\, \mathfrak{E}(r)^{1-e},$$

so erhält man daraus den Satz:

5. Eine Normaleinheit des Körpers H_m, die mit ihren Conjugirten gleiches Vorzeichen hat, ist, vom Vorzeichen abgesehen, ein Quadrat einer Normaleinheit.

§. 201.

Fundamentalsystem von Einheiten des Körpers H_m.

Es bleibt noch übrig, den Nenner D in der Formel für B [§. 197, (6)] zu bestimmen, der durch die Gleichung

$$E = E'D$$

definirt war, worin E und E' die Regulatoren der Körper H_m, H_μ bedeuteten.

Hier handelt es sich also nicht mehr um die Normaleinheiten, sondern um die Einheiten des Körpers H_m überhaupt.

Wir nehmen ein Fundamentalsystem von Einheiten im Körper H_m an:

(1) $$\varepsilon_1(r_i),\ \varepsilon_2(r_i),\ \ldots,\ \varepsilon_{\nu-1}(r_i),$$

und die conjugirten Logarithmen dieses Systems seien:

(2) $$l_{1,k},\ l_{2,k},\ \ldots,\ l_{\nu-1,k} \quad k = 0, 1, 2, \ldots, \nu - 1.$$

Daneben betrachten wir ein Fundamentalsystem im Körper H_μ

(3) $$\varepsilon'_1,\ \varepsilon'_2,\ \ldots,\ \varepsilon'_{\nu'-1}$$

mit den conjugirten Logarithmen

(4) $$l'_{1,k},\ l'_{2,k},\ \ldots,\ l'_{\nu'-1,k} \quad k = 0, 1, 2, \ldots, \nu' - 1.$$

Bei der Bildung der Regulatoren wird einer der conjugirten Werthe, etwa $k = 0$, weggelassen (vgl. §. 186), und wir erhalten daher

(5) $$\begin{aligned} E &= \pm \Sigma \pm l_{1,1}\, l_{2,2} \ldots l_{\nu-1,\nu-1} \\ E' &= \pm \Sigma \pm l'_{1,1}\, l'_{2,2} \ldots l'_{\nu'-1,\nu'-1}. \end{aligned}$$

Nun fügen wir zu dem Systeme (3) ein Fundamentalsystem von Normaleinheiten des Körpers H_m

(6) $$\mathfrak{E}_0,\ \mathfrak{E}_1,\ \ldots,\ \mathfrak{E}_{\nu'-1},$$

und wir behaupten, dass das System

(7) $$\varepsilon'_1,\ \varepsilon'_2,\ \ldots,\ \varepsilon'_{\nu'-1},\ \mathfrak{E}_0,\ \mathfrak{E}_1,\ \ldots,\ \mathfrak{E}_{\nu'-1}$$

ein unabhängiges System von Einheiten des Körpers H_m ist (wenn auch nicht ein Fundamentalsystem).

Bezeichnen wir mit

(8) $$L_{0,k},\ L_{1,k},\ \ldots,\ L_{\nu'-1,k} \quad k = 0, 1, \ldots, \nu' - 1$$

die conjugirten Logarithmen des Systems (6), so ist nach dem vorigen Paragraphen

(9) $$\pm \Sigma \pm L_{0,0}\, L_{1,1} \ldots L_{\nu'-1,\nu'-1} = T_0$$

der Regulator dieses Systems, und wir haben mit Rücksicht auf die Definition der Normaleinheiten [§. 200, (9)]:

(10) $$L_{i,k+\nu'} = -L_{i,k},$$

und weil die ε'_i als Zahlen des Körpers H_μ durch die Substitution $(r, -r)$ ungeändert bleiben:

(11) $$l'_{i,k+\nu'} = l'_{i,k}.$$

Hiernach ergiebt sich der Regulator R des Systems (7) aus der Determinante:

$$\begin{vmatrix} l'_{1,1}, & l'_{2,1}, & \ldots, & l'_{\nu'-1,1}, & L_{0,1}, & L_{1,1}, & \ldots, & L_{\nu'-1,1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ l'_{1,\nu'-1}, & l'_{2,\nu'-1}, & \ldots, & l'_{\nu'-1,\nu'-1}, & L_{0,\nu'-1}, & L_{1,\nu'-1}, & \ldots, & L_{\nu'-1,\nu'-1} \\ l'_{1,0}, & l'_{2,0}, & \ldots, & l'_{\nu'-1,0}, & -L_{0,0}, & -L_{1,0}, & \ldots, & -L_{\nu'-1,0} \\ l'_{1,1}, & l'_{2,1}, & \ldots, & l'_{\nu'-1,1}, & -L_{0,1}, & -L_{1,1}, & \ldots, & -L_{\nu'-1,1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ l'_{1,\nu'-1}, & l'_{2,\nu'-1}, & \ldots, & l'_{\nu'-1,\nu'-1}, & -L_{0,\nu'-1}, & -L_{1,\nu'-1}, & \ldots, & -L_{\nu'-1,\nu'-1} \end{vmatrix}.$$

Diese Determinante hat $\nu - 1$ Zeilen; wir addiren die erste zur $(\nu'+1)^{\text{ten}}$, die zweite zur $(\nu'+2)^{\text{ten}}$ u. s. f., die $(\nu'-1)^{\text{te}}$ zur letzten. Dadurch heben sich in den letzten $(\nu'-1)$ Zeilen die L heraus und die l bekommen den Factor 2 [nach (10), (11)], und hieraus ergiebt sich nach einem Determinantensatze (Bd. I, §. 23, V.):

$$R = 2^{\nu'-1} E' T_0. \tag{12}$$

Da hiernach R nicht verschwindet und daher in (7) ein System von $\nu - 1$ unabhängigen Einheiten des Körpers H_m vorliegt, so können wir [nach §. 186, (5)] die rationalen (ganzen oder gebrochenen) Zahlen $m_{i,k}$, $M_{i,k}$ aus den Gleichungen

$$\begin{aligned} 2\, l_{i,k} = {} & m_{1,i}\, l'_{1,k} + \cdots + m_{\nu'-1,i}\, l'_{\nu'-1,k} \\ & + M_{0,i}\, L_{0,k} + M_{1,i}\, L_{1,k} + \cdots + M_{\nu'-1,i}\, L_{\nu'-1,k} \end{aligned} \tag{13}$$

bestimmen. Es lässt sich aber leicht durch die Relationen (10), (11) nachweisen, dass die Zahlen $m_{i,k}$, $M_{i,k}$ hier ganze sein müssen. Denn es ist

$$\begin{aligned} l_{i,k} + l_{i,k+\nu'} &= \log |\varepsilon_i(r_k)\, \varepsilon_i(-r_k)| = \\ & m_{1,i}\, l'_{1,k} + \cdots + m_{\nu'-1,i}\, l'_{\nu'-1,k} \\ l_{i,k} - l_{i,k+\nu'} &= \log |\varepsilon_i(r_k)\, \varepsilon_i(-r_k)^{-1}| = \\ & M_{0,i} L_{0,k} + M_{1,i} L_{1,k} + \cdots + M_{\nu'-1,i} L_{\nu'-1,k}. \end{aligned}$$

Die Einheiten $\varepsilon_i(r)\, \varepsilon_i(-r)$ gehören aber dem Körper H_u an, und da die ε'_i nach Voraussetzung ein Fundamentalsystem dieses Körpers sind, so müssen die $m_{i,k}$ nach §. 187 ganze rationale Zahlen sein.

Die Einheiten $\varepsilon_i(r)\, \varepsilon_i(-r)^{-1}$ sind Normaleinheiten des Körpers H_m, und weil die $\mathfrak{E}_i$ ein Fundamentalsystem von Normaleinheiten sein sollten, so sind nach §. 200 die $M_{i,k}$ ganze Zahlen.

Zur besseren Uebersicht setzen wir die Gleichungen (13) noch einmal ohne den Index k, der die conjugirten Werthe von einander unterscheidet, hierher:

$$(14)\qquad 2l_i = m_{1,i}l'_1 + m_{2,i}l'_2 + \cdots + m_{\nu'-1,i}l'_{\nu'-1} + M_{0,i}L_0 + M_{1,i}L_1 + M_{2,i}L_2 + \cdots + M_{\nu'-1,i}L_{\nu'-1}.$$

Bilden wir nun nach (13) den Regulator E und bezeichnen mit M den absoluten Werth der Determinante der $\nu - 1$ Reihen der Zahlen $m_{k,i}$, $M_{k,i}$:

$$M = \pm \Sigma \pm m_{1,1} \ldots m_{\nu'-1,\nu'-1} M_{0,0} M_{1,1} \ldots M_{\nu'-1,\nu'-1},$$

so folgt:

$$(15)\qquad 2^{\nu-1}E = MR,$$

und daraus mit Rücksicht auf (12):

$$(16)\qquad E = 2^{-\nu} M E' T_0.$$

Es lässt sich nun weiter nachweisen, dass M eine Potenz von 2 und durch $2^{\nu'}$ theilbar ist.

Da nämlich das System (1) als Fundamentalsystem in H_m vorausgesetzt war, so giebt es ganze rationale Zahlen $n_{k,i}$, $N_{k,i}$, die den Gleichungen genügen:

$$(17)\qquad \begin{aligned} l'_i &= n_{1,i}l_1 + n_{2,i}l_2 + \cdots + n_{\nu-1,i}l_{\nu-1}, \quad i = 1, 2, \ldots, \nu' - 1 \\ L_i &= N_{1,i}l_1 + N_{2,i}l_2 + \cdots + N_{\nu-1,i}l_{\nu-1}, \quad i = 0, 1, 2, \ldots, \nu' - 1. \end{aligned}$$

Bilden wir daraus die Determinante R und bezeichnen mit N den absoluten Werth der Determinante der $n_{k,i}$, $N_{k,i}$, so folgt:

$$R = NE,$$

und daraus nach (15):

$$MN = 2^{\nu-1};$$

daraus folgt, dass jede der beiden ganzen Zahlen M, N eine Potenz von 2 sein muss.

Um zu entscheiden, durch welche Potenz von 2 die Determinante M theilbar ist, bestimmen wir zunächst ein System ganzer rationaler Zahlen a_i ohne gemeinschaftlichen Theiler, das den linearen Gleichungen

$$(18)\qquad \sum_{1,\nu-1}^{i} a_i m_{k,i} = 0 \quad (k = 1, 2, \ldots, \nu' - 1)$$

genügt. Setzen wir dann

$$\sum_{1,\nu-1}^{i} a_i M_{k,i} = \xi_k,$$

so erhalten wir aus den Gleichungen (13)

$$2 \sum_{1, \nu-1}^{i} a_i l_{i,k} = \xi_0 L_{0,k} + \xi_1 L_{1,k} + \cdots + \xi_{\nu'-1} L_{\nu'-1,k}.$$

Daraus ergiebt sich nach (10)

$$\sum^{i} a_i l_{i,k+\nu'} = - \sum a_i l_{i,k},$$

und dies bedeutet, dass

$$\delta = \varepsilon_1^{a_1} \varepsilon_2^{a_2} \dots \varepsilon_{\nu-1}^{a_{\nu-1}}$$

eine Normaleinheit des Körpers H_m ist. Daraus folgt dann weiter, weil $\mathfrak{E}_0, \mathfrak{E}_1, \dots, \mathfrak{E}_{\nu'-1}$ ein Fundamentalsystem von Normaleinheiten ist, dass die Zahlen $\xi_0, \xi_1, \dots, \xi_{\nu'-1}$ gerade sein müssen. Daraus ergiebt sich:

1. Das System der Gleichungen (18) hat die Congruenzen

$$\sum_{1, \nu-1}^{i} a_i M_{k,i} \equiv 0 \pmod 2 \qquad k = 0, 1, \dots, \nu'-1 \tag{19}$$

zur Folge.

In den Gleichungen (18), deren Anzahl nur $\nu' - 1$ beträgt, sind aber $\nu - 1$ Unbekannte a_i enthalten. Daher giebt es mehrere Systeme von einander unabhängiger Lösungen, was wir etwas genauer dahin präcisiren können:

2. Es giebt ν' ganzzahlige Lösungen des Systems (18):

$$\begin{matrix} a_{1,1}, & a_{2,1}, & \dots, & a_{\nu-1,1} \\ a_{1,2}, & a_{2,2}, & \dots, & a_{\nu-1,2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1,\nu'}, & a_{2,\nu'}, & \dots, & a_{\nu-1,\nu'} \end{matrix} \tag{20}$$

von der Art, dass aus der Matrix (20) eine Determinante von ν' Reihen gebildet werden kann, die eine ungerade Zahl ist.

Denn es giebt zunächst eine Lösung von (18):

$$a_{1,1}, a_{2,1}, a_{3,1}, \dots, a_{\nu-1,1},$$

in der eine ungerade Zahl vorkommt. Nehmen wir an, was gestattet ist, da hier auf die Anordnung der Indices nichts an-

kommt, es sei $a_{1,1}$ diese ungerade Zahl, dann bestimmen wir eine zweite Lösung:

$$0,\ a_{2,2},\ a_{3,2},\ \ldots,\ a_{\nu-1,2},$$

in der wieder eine ungerade Zahl, etwa $a_{2,2}$, vorkommt. Dann bestimmen wir eine dritte Lösung:

$$0,\ 0,\ a_{3,3},\ \ldots,\ a_{\nu-1,3},$$

und fahren mit Nullsetzen so lange fort, als die Anzahl der übrig bleibenden Unbekannten noch grösser ist, als die Anzahl der Gleichungen.

Im letzten Systeme werden also $\nu' - 1$ Nullen vorkommen, damit ν' Unbekannte übrigbleiben.

Diese Zahlenreihen $a_{\nu,k}$ können wir für das System (20) setzen, denn darin reducirt sich die Determinante

$$(21) \qquad \Sigma \pm a_{1,1}\, a_{2,2} \ldots a_{\nu',\nu'}$$

auf das Diagonalglied $a_{1,1}\, a_{2,2} \ldots a_{\nu',\nu'}$, dessen Factoren alle ungerade sind.

Ist nun die Forderung des Satzes 2. erfüllt, so lässt sich die Matrix (20) durch Hinzufügung von $\nu' - 1$ Zeilen zu einer Determinante von $\nu - 1$ Reihen ergänzen, die gleichfalls einen ungeraden ganzzahligen Werth hat:

$$(22) \qquad a = \Sigma \pm a_{1,1}\, a_{2,2} \ldots a_{\nu',\nu'}\, a_{\nu'+1,\nu'+1} \ldots a_{\nu-1,\nu-1}.$$

Man braucht nur, wenn die Determinante (21) als ungerade vorausgesetzt wird, in den hinzugefügten Zeilen für die Elemente lauter Nullen zu setzen, ausgenommen die in der Diagonalreihe stehenden, $a_{\nu'+1,\nu'+1} \ldots a_{\nu-1,\nu-1}$, die gleich 1 genommen werden können. Dann erhält a denselben Werth wie die Determinante (21).

Wenn wir aber jetzt nach dem Multiplicationssatze der Determinanten das Product $a\,M$ bilden, so ergiebt sich eine Determinante, in der die $\nu - 1$ Summen

$$\sum_{1,\nu-1}^{i} a_{i,s}\, m_{k,i}, \qquad \sum_{1,\nu-1}^{i} a_{i,s}\, M_{k,i}$$

$$k = 1, 2, \ldots \nu' - 1, \quad k = 0, 1, 2 \ldots \nu' - 1$$

für jeden Werth $s = 1, 2, \ldots, \nu'$ eine Reihe bilden, und in der also ν' Reihen vorkommen, deren Elemente alle durch 2 theilbar sind.

Demnach ist aM und folglich auch M durch $2^{\nu'}$ theilbar, und wenn wir

(23) $$M = 2^{\nu'+\sigma}, \quad N = 2^{\nu'-\sigma-1}$$

setzen, so ist σ eine nicht negative ganze rationale Zahl.

Setzen wir dies in (16) ein, so folgt:

$$E = 2^{\sigma} E' T_0.$$

Nun war in §. 197, (6)

$$E = E' D$$

gesetzt, und es ergiebt sich also:

$$D = 2^{\sigma} T_0.$$

Hieraus folgt für den Classenzahlfactor B nach §. 199, (15) und §. 200, (21):

(24) $$B = 2^{-\sigma} \frac{T}{T_0} = 2^{-\sigma} C,$$

worin C eine ungerade ganze Zahl ist.

Demnach ergiebt sich nach §. 197, (4) für den zweiten Factor der Classenzahl h_1, der, wie wir gesehen haben, eine ganze Zahl ist:

(25) $$h_1 = 2^{-\sigma} h_1' C.$$

Nehmen wir nun als bewiesen an, dass h_1' ungerade ist, so folgt, da auch C ungerade ist, dass $\sigma = 0$ und h_1 ungerade ist, und beides ist also damit durch vollständige Induction bewiesen.

Damit werden die abgeleiteten Resultate folgendermaassen vereinfacht:

3. Es ist

(26) $$M = 2^{\nu'}, \quad D = T_0, \quad B = \frac{T}{T_0};$$

der Classenzahlfactor B ist gleich dem Verhältniss des Regulators T der Einheiten τ zum Regulator T_0 eines Fundamentalsystems von Normaleinheiten, und ist eine ungerade ganze Zahl.

Bezeichnen wir die zu $m = 2^{\varkappa}$ gehörige Zahl B mit $B_{\varkappa}$, so ist die Classenzahl h_1, wie durch vollständige Induction folgt,

(27) $$h_1 = B_4 B_5 \ldots B_{\varkappa},$$

und ist also auch eine ungerade Zahl. Damit ist dann, mit Rücksicht auf §. 198, 1., das Haupttheorem bewiesen:

A. Die Classenzahl im Körper Ω_m ist, wenn m eine Potenz von 2 ist, ungerade.

§. 202.

Positive Einheiten.

Die zuletzt gefundenen Resultate zeigen, dass das System unabhängiger Einheiten §. 201, (7)

$$\varepsilon_1', \varepsilon_2', \ldots, \varepsilon_{\nu'-1}', \mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\nu'-1}$$

im Körper H_m **kein Fundamentalsystem** bildet. Denn sonst müssten in den Formeln §. 201, (13) die Zahlen $m_{k,i} M_{k,i}$ sämmtlich durch 2 theilbar sein, und es wäre die Determinante M, deren Werth wir $= 2^{\nu'}$ gefunden haben, durch $2^{\nu-1}$ theilbar.

Wir betrachten nun an Stelle des Systems der Gleichungen (18), §. 201 die folgenden Congruenzen:

$$(1) \qquad \begin{aligned} &\sum_{1,\nu-1}^{i} b_i m_{1,i} \equiv 1 \\ &\sum_{1,\nu-1}^{i} b_i m_{2,i} \equiv 0 \pmod 2, \\ &\ldots\ldots\ldots\ldots \\ &\sum_{1,\nu-1}^{i} b_i m_{\nu'-1,i} \equiv 0 \end{aligned}$$

und beweisen, dass es möglich ist, ihnen durch ganzzahlige Werthe der b_i zu genügen.

Wäre es nicht möglich, so müsste sich aus den $\nu' - 2$ Congruenzen

$$\sum_{1,\nu-1}^{i} b_i m_{k,i} \equiv 0 \pmod 2 \quad k = 2, 3, \ldots, \nu' - 1$$

die letzte

$$\sum_{1,\nu-1}^{i} b_i m_{1,i} \equiv 0 \pmod 2$$

als **Folgerung** ergeben, und dann würde, wie im vorigen Paragraphen, weiter folgen:

$$\sum_{1,\nu-1}^{i} b_i M_{k,i} \equiv 0 \pmod 2 \quad k = 0, 1, \ldots, \nu' - 1.$$

Man könnte dann an Stelle der Matrix §. 201, (20) eine Matrix der $b_{k,i}$ von $\nu' + 1$ Reihen setzen, und es würde sich auf dem im vorigen Paragraphen eingeschlagenen Wege schliessen lassen, dass M durch $2^{\nu'+1}$ theilbar sein müsste, was nicht der Fall ist.

Wenden wir aber das System der Multiplicatoren b_i, das den Bedingungen (1) genügt, auf die Gleichungen (14) des vorigen Paragraphen an, indem wir mit b_i multipliciren und dann summiren, so ergiebt sich, wenn wir Vielfache von 2 weglassen und dies auch hier (wo irrationale Zahlen, nämlich die Logarithmen, auftreten) durch das Zeichen der Congruenz ausdrücken:

$$(2) \qquad l'_1 \equiv L_0 \Sigma M_{0,i} b_i + L_1 \Sigma M_{1,i} b_i + \cdots + L_{\nu'-1} \Sigma M_{\nu'-1,i} b_i \pmod 2.$$

Wollen wir die Congruenz in eine Gleichung verwandeln, so kommt eine Summe von Grössen

$$l_1, l_2, \ldots, l_{\nu-1}, \quad l'_1, l'_2, \ldots, l'_{\nu'-1}$$

mit geraden ganzen Zahlen als Coëfficienten hinzu.

Dieselbe Betrachtung lässt sich aber auf $l'_2, l'_3, \ldots, l'_{\nu'-1}$ anwenden, und danach kann man, wenn man von den Logarithmen wieder zu den Zahlen übergeht, die Formel (2) so in Worte fassen:

1. Jede Einheit des Körpers H_μ ist als Product einer Normaleinheit des Körpers H_m und eines Quadrates einer Einheit in H_m darstellbar.

Wenn wir darauf den Satz 2., §. 200 anwenden, so ergiebt sich, dass jede Einheit $\mathcal{E}(r)$ des Körpers H_μ, die mit allen ihren Conjugirten dasselbe Zeichen hat, vom Vorzeichen abgesehen, das Quadrat einer Einheit in H_m sein muss. Ist aber

$$\pm \mathcal{E}(r) = \Delta(r)^2,$$

worin $\mathcal{E}(r)$ eine Einheit in H_μ und $\Delta(r)$ eine Einheit in H_m ist, so muss auch $\Delta(r)$ in H_μ enthalten sein.

Denn setzen wir

$$\Delta(r) = \Delta_1(r^2) + r\Delta_2(r^2),$$

so kann das Quadrat davon nur dann in H_μ enthalten sein, also durch die Vorzeichenänderung von r ungeändert bleiben, wenn entweder Δ_1 oder $\Delta_2 = 0$ ist. Es kann aber nicht $\Delta(r) = r\Delta_2(r^2)$ sein, denn sonst wäre $\Delta_2(r^2)$ eine Einheit in Ω_μ und müsste

nach §. 178, 1. das Product einer reellen Einheit und einer Einheitswurzel $r^{2\lambda}$ sein, und da auch $\Delta(r)$ reell ist, so müsste $r^{2\lambda+1}$ reell sein, was nicht möglich ist. Demnach ist $\Delta(r)$ in H_μ enthalten.

Da nun μ ebenso wie m jede beliebige Potenz von 2 sein kann, so ergiebt sich hieraus das zweite Haupttheorem:

B. Eine Einheit des Körpers H_m, die mit allen ihren Conjugirten positiv ist, ist das Quadrat einer Einheit desselben Körpers.

Von den beiden Theoremen A. und B. haben wir aber im §. 184 den Beweis des Hauptsatzes von den Abel'schen Zahlkörpern (§. 179, I.) abhängig gemacht.

Fünfundzwanzigster Abschnitt.

Transcendente Zahlen.

---

§. 203.

Abzählbare Mengen.

In der Einleitung zu unserem Werke ist der allgemeine Begriff der Zahlen definirt worden, und mit diesem allgemeinen Zahlbegriffe haben wir zunächst, z. B. bei dem Beweise der Wurzelexistenz, operirt. Im weiteren Verlaufe unserer Betrachtungen haben wir uns dann nur mit algebraischen Zahlen beschäftigt, ohne uns darüber Rechenschaft zu geben, ob damit der Umfang des Zahlenbereiches erschöpft sei, oder ob es auch nichtalgebraische Zahlen giebt. Die Existenz von nichtalgebraischen Zahlen, die man auch transcendente Zahlen nennt, ist zuerst von Liouville bewiesen. Andere Beweise für diesen Satz rühren von G. Cantor her[1]).

Wir knüpfen hier an den schon in der Einleitung aus einander gesetzten Begriff einer Menge oder Mannigfaltigkeit an, worunter ein System von Elementen irgend welcher Art zu verstehen ist, was so genau abgegrenzt ist, dass von jedem beliebigen Objecte völlig entschieden ist, ob es zu dem Systeme gehört oder nicht.

Wir unterscheiden endliche und unendliche Mengen, und führen als erstes und wichtigstes Beispiel einer unendlichen Menge die Gesammtheit der natürlichen Zahlen $1, 2, 3, \ldots$ an. Dann gilt folgende Definition:

1. **Definition.** Eine Menge heisst abzählbar, wenn ihre Elemente mit der natürlichen Zahlenreihe

---

[1]) G. Cantor, Crelle's Journal, Bd. 77 (1873). Ueber eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen.

oder einem Theil derselben in eine gegenseitig eindeutige Beziehung gesetzt werden kann[1]).

Jede endliche Menge ist hiernach abzählbar, und bei der Abzählung wird die natürliche Zahlenreihe nur bis zu einer gewissen höchsten Zahl verwendet. Im Weiteren betrachten wir vorzugsweise unendliche Mengen.

Wir können der Definition für eine unendliche abzählbare Menge auch den Ausdruck geben, dass es eine solche Menge ist, bei der jedem Elemente eine bestimmte Zahl der natürlichen Zahlenreihe als Name beigelegt werden kann, so dass auch jede Zahl der Zahlenreihe dabei verwandt wird, also eine Menge, in der es ein erstes, zweites, drittes ... hundertstes ... Element giebt.

Endlich können wir auch sagen, dass eine unendliche abzählbare Menge eine solche ist, die sich derart in eine Reihe ordnen lässt, dass ein erstes Element vorhanden ist, und dass auf jedes Element ein bestimmtes anderes der Menge folgt, und jedem Elemente, mit Ausnahme des ersten, ein bestimmtes anderes Element vorangeht. Eine solche Reihe können wir eine zählbare Anordnung nennen.

Es ist klar, dass eine abzählbare Menge nicht nur auf eine, sondern auf unendlich viele verschiedene Arten abzählbar ist.

Ausser der natürlichen Zahlenreihe selbst, die sicher abzählbar ist, können wir als zweites Beispiel das System der rationalen positiven echten Brüche anführen, die unter Anderem in folgender Weise abgezählt werden können:

$$\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{1}{6}, \frac{5}{6}, \ldots$$

d. h. so, dass jeder grössere Nenner dem kleineren Nenner folgt, und dass die Brüche von gleichem Nenner nach der Grösse des Zählers geordnet sind. Wollte man aber die Brüche nach der Grösse ihres numerischen Werthes ordnen, so würde man keine zählbare Anordnung bekommen.

2. Die Gesammtheit aller algebraischen Zahlen ist eine abzählbare Menge.

---

[1]) Cantor, l. c. Der Begriff der abzählbaren Mengen deckt sich mit dem von Dedekind ohne die Voraussetzung des Zahlensystems definirten Begriffe der einfach unendlichen Systeme. (Dedekind, Was sind und was sollen die Zahlen? §. 6. Braunschweig 1887. Zweite unveränderte Auflage 1893.)

Um diesen wichtigen Satz nachzuweisen, erinnern wir uns daran, dass jede algebraische Zahl Θ die Wurzel einer und nur einer irreduciblen Gleichung

$$(1) \qquad f(\Theta) = a_0 \Theta^n + a_1 \Theta^{n-1} + \cdots + a_n = 0$$

ist, in der $a_0, a_1, \ldots, a_n$ ganze rationale Zahlen ohne gemeinsamen Theiler sind, und a_0 von Null verschieden und positiv ist. Der Grad n der Gleichung (1) ist eine positive ganze Zahl, also mindestens $= 1$. Die Zahlen $a_1, \ldots, a_{n-1}$ können zum Theil Null sein.

Wir wollen nun die Vorzeichen $\pm$ so bestimmen, dass $\pm a_1$, $\pm a_2, \pm a_3, \ldots, \pm a_n$ nicht negativ sind, und nennen die Summe

$$(2) \qquad N = (n-1) + a_0 \pm a_1 \pm a_2 \cdots \pm a_n$$

die Höhe der algebraischen Zahl Θ. Die Höhe ist dann immer eine positive ganze Zahl.

Nun ist leicht zu sehen, dass es für einen gegebenen Werth der Höhe N immer nur eine endliche Anzahl von algebraischen Zahlen geben kann. Denn zunächst kann n nach (2) niemals grösser als N sein, und zu jedem gegebenen N und n können die Zahlen $a_0, a_1, \ldots, a_n$ nur auf eine endliche Anzahl von Arten bestimmt werden. Man hat dann unter den so bestimmten Functionen $f(\Theta)$ nur die irreduciblen beizubehalten. Wenn man nun die algebraischen Zahlen in der Weise ordnet, dass man die Zahlen von geringerer Höhe denen von grösserer Höhe voranstellt, dass man unter Zahlen gleicher Höhe die voranstellt, deren reeller Theil kleiner ist, und unter Zahlen von gleicher Höhe und gleichem reellen Theile die von kleinerem imaginären Theile vorangehen lässt, so haben wir eine zählbare Anordnung der algebraischen Zahlen, und es ist erwiesen, dass die Gesammtheit aller algebraischen Zahlen eine abzählbare Menge ist.

Wir erhalten beispielsweise:

$$\begin{array}{llll} N = 1, & n = 1, & a_0 = 1, & a_1 = 0 \\ N = 2, & n = 1, & a_0 = 1, & a_1 = \pm 1 \\ N = 3, & n = 1, & a_0 = 1, & a_1 = \pm 2 \\ & & a_0 = 2, & a_1 = \pm 1 \\ & n = 2, & a_0 = 1, & a_1 = 0, \quad a_2 = 1, \end{array}$$

und der Anfang der geordneten Reihe der algebraischen Zahlen wird also:

$$0, \; -1, \; +1, \; -2, \; -\tfrac{1}{2}, \; -\sqrt{-1}, \; \sqrt{-1}, \; \tfrac{1}{2}, \; 2, \ldots$$

Jeder Theil der natürlichen Zahlenreihe ist eine abzählbare Menge; denn man braucht ja die Zahlen eines solchen Theiles nur nach ihrer Grösse zu ordnen, um eine zählbare Anordnung zu erhalten.

Daraus aber ergiebt sich, dass jeder Theil einer abzählbaren Menge selbst eine abzählbare Menge ist. Es folgt daraus unter Anderem, dass auch die Menge der reellen algebraischen Zahlen abzählbar ist.

§. 204.

Unzählbare Mengen.

Wir kommen nun zweitens zu dem Beweise des Satzes, dass es unter den Zahlenmengen auch nicht abzählbare giebt, und wir werden speciell nachweisen:

Dass die Gesammtheit aller reellen Zahlen, selbst wenn wir uns auf ein endliches Intervall beschränken, nicht abzählbar ist.

Wir betrachten zu diesem Zwecke irgend eine abzählbare Menge reeller von einander verschiedener Zahlen, die wir, in eine zählbare Anordnung Ω gesetzt, so bezeichnen wollen:

$$(\Omega) \qquad \omega_1, \omega_2, \omega_3, \omega_4, \ldots$$

(wobei daran zu erinnern ist, dass dies nicht etwa eine Aufeinanderfolge nach der Grösse bedeuten soll).

Der Kürze wegen wollen wir von zwei Elementen der Reihe Ω das mit kleinerem Index das frühere, das mit grösserem das spätere nennen.

Wir nehmen nun irgend zwei reelle Zahlen α, β an, so dass $\alpha < \beta$ ist, und zeigen, dass es in dem Intervalle $\delta = (\alpha, \beta)$ mindestens eine Zahl giebt, die nicht in der Reihe Ω vorkommt. Haben wir eine solche Zahl für jedes Intervall nachgewiesen, so giebt es auch deren unendlich viele, da man ja dieselbe Schlussweise auf jeden Theil des Intervalles (α, β) anwenden kann.

Zunächst ist klar, dass unsere Behauptung richtig ist, wenn in irgend einem endlichen Theile des Intervalles δ nur eine endliche Anzahl von Zahlen der Reihe Ω enthalten ist, und wir können also ohne Weiteres zu dem Falle übergehen, dass in jedem noch so kleinen Theile des Intervalles δ eine unendliche Menge von Zahlen der Reihe Ω liegt.

Wir bezeichnen mit α_1, β_1 die beiden frühesten Zahlen der Reihe Ω, die in dem Intervalle δ liegen, nehmen $\alpha_1 < \beta_1$ an, und setzen $\delta_1 = \beta_1 - \alpha_1$, so dass $\delta_1 = (\alpha_1, \beta_1)$ ein Theil des Intervalles δ ist.

Nun bezeichnen wir ebenso mit α_2, β_2 die beiden frühesten Zahlen von Ω, die im Inneren des Intervalles δ_1 (mit Ausschluss der Grenzen) liegen, setzen $\alpha_2 < \beta_2$ voraus, und setzen $\delta_2 = \beta_2 - \alpha_2$.

Auf diese Weise können wir fortfahren und erhalten eine unbegrenzte Reihe von Intervallen:

$$\delta, \delta_1, \delta_2, \delta_3, \ldots,$$

deren jedes alle folgenden einschliesst, und zwei Reihen von Zahlen:

$$\alpha, \alpha_1, \alpha_2, \ldots$$
$$\beta, \beta_1, \beta_2, \ldots$$

die, mit etwaiger Ausnahme der ersten, α und β, alle der Reihe Ω angehören. Die $\alpha, \alpha_1, \alpha_2, \ldots$ bilden eine wachsende, die $\beta, \beta_1, \beta_2, \ldots$ eine fallende Zahlenreihe, und zugleich ist jedes α kleiner als jedes β.

1. Daraus ergiebt sich, dass die Zahlen α_ν eine obere Grenze a, die Zahlen β_ν eine untere Grenze b haben, und dass a jedenfalls nicht grösser als b ist. (Vgl. Bd. I, §. 38, 1.)

Es kann aber möglicherweise $a = b$ sein.

Aus der Bildungsweise der Intervalle $\delta, \delta_1, \delta_2, \ldots$ geht noch Folgendes hervor:

2. Wenn irgend eine Zahl ω der Reihe Ω in dem Intervalle δ_ν, mit Ausschluss seiner Grenzen α_ν, β_ν, liegt, so ist ω in der Reihe Ω später als das derselben Reihe angehörige Zahlenpaar α_ν, β_ν.

Denn α_ν, β_ν waren ja die beiden frühesten im Intervalle $\delta_{\nu-1}$ gelegenen Zahlen von Ω. Daraus folgt:

3. Die der Reihe Ω angehörigen Zahlenpaare α_ν, β_ν sind um so spätere Glieder der Reihe Ω, je grösser der Index ν ist, und da wir angenommen haben, die Reihe der Intervalle δ_ν breche nicht ab, so können wir α_ν, β_ν für ein hinlänglich grosses ν beliebig weit in der Reihe Ω hinausrücken lassen.

Nun ergiebt sich sehr einfach, dass keine Zahl g, die mit einer der Zahlen a, b zusammenfällt, oder auch, wenn a und b verschieden sind, zwischen ihnen liegt, zu der Reihe Ω gehören kann.

Denn die Zahl g liegt im Inneren eines jeden der Intervalle δ_ν. Nehmen wir an, es komme g in Ω vor, und gehen nach 3. mit ν so weit, dass α_ν, β_ν in Ω später als g kommt, so kann g nach 2. nicht im Intervall δ_ν liegen, und damit ist die Unmöglichkeit unserer Annahme erwiesen.

Daraus folgt also, dass die Gesammtheit der Zahlen eines Intervalles α, β keine abzählbare Menge bildet.

Diese Thatsache lässt sich noch auf einem anderen Wege beweisen, der in gewisser Beziehung noch einfacher ist und den wir mit wenig Worten darlegen wollen. Wir beschränken die Allgemeinheit nicht, wenn wir das Intervall von 0 bis 1 zu Grunde legen. Alle Zahlen dieses Intervalles denken wir uns durch unendliche Decimalbrüche dargestellt. Darunter sind auch die endlichen Decimalbrüche enthalten, wenn wir alle Ziffern, von einer gewissen an, gleich Null setzen. Um die Darstellung durch Decimalbrüche zu einer eindeutigen zu machen, mag noch festgesetzt sein, dass für einen endlichen Decimalbruch immer diese Darstellung gewählt, also z.B. nicht 0,4999 ... für 0,5000 ... gesetzt werden soll.

Wir wollen nun annehmen, diese Decimalbrüche bilden eine abzählbare Menge; sie lassen sich also in eine zählbare Reihe anordnen, die wir so darstellen:

$$(\Omega) \qquad \begin{aligned} \omega_1 &= 0,\, \alpha_1^{(1)}\, \alpha_2^{(1)}\, \alpha_3^{(1)} \ldots \\ \omega_2 &= 0,\, \alpha_1^{(2)}\, \alpha_2^{(2)}\, \alpha_3^{(2)} \ldots \\ \omega_3 &= 0,\, \alpha_1^{(3)}\, \alpha_2^{(3)}\, \alpha_3^{(3)} \ldots \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

worin die $\alpha_\mu^{(\nu)}$ Ziffern des dekadischen Systems bedeuten.

Es ist nun aber sehr leicht, einen Decimalbruch (oder auch beliebig viele) nachzuweisen, die in der Reihe Ω nicht enthalten sind. Wir brauchen nur

$$\eta = 0,\, \beta_1\, \beta_2\, \beta_3 \ldots$$

zu bilden, wobei die β_ν Ziffern des dekadischen Systems sind, die der einen Bedingung genügen, dass β_ν für jedes ν von $\alpha_\nu^{(\nu)}$ ver-

schieden ist. Diese Zahl η, die doch auch dem Intervalle (0, 1) angehört, kann mit keiner Zahl der Reihe Ω übereinstimmen.

Man kann die Bildung von η noch dadurch verallgemeinern, dass man die ersten β bis zu einem beliebig weit entfernten willkürlich annimmt, und erst von da an das Gesetz: β_ν verschieden von $\alpha_\nu^{(\nu)}$, gelten lässt.

Da nun bewiesen ist, dass die reellen algebraischen Zahlen eine abzählbare Menge bilden, und dass es in jedem Intervalle Zahlen giebt, die einer gegebenen abzählbaren Menge nicht angehören, so folgt hieraus ganz unmittelbar:

Es giebt in jedem reellen Intervalle transcendente Zahlen.

§. 205.

Transcendenz der Zahl e.

Eine weit schwierigere Aufgabe ist es nun, von einer bestimmt vorgelegten Zahl zu entscheiden, ob sie algebraisch oder transcendent ist. Hier hat sich das Interesse hauptsächlich auf die beiden in der Analysis so häufig vorkommenden Zahlen e, d. h. die Basis des natürlichen Logarithmensystems, und die Ludolph'sche Zahl π, das Verhältniss des Kreisumfanges zum Durchmesser, concentrirt.

Für die Zahl e ist die Frage von Hermite in einer berühmten Abhandlung entschieden, die für die späteren Untersuchungen über die Zahl π die Grundlage geworden ist [1]). Die Entscheidung für die Zahl π, die wegen ihrer Beziehung zu dem altberühmten Problem der Quadratur des Kreises ganz besonders interessant war, bot aber noch lange Zeit unüberwindliche Schwierigkeiten. Endlich ist von Lindemann der Nachweis geführt, dass auch π zu den transcendenten Zahlen gehört. Der von Lindemann gegebene Beweis bot aber dem Verständniss zunächst noch grosse Schwierigkeiten, die durch spätere Untersuchungen von Weierstrass, Hilbert, Hurwitz und Gordan [2])

1) Hermite, Sur la fonction exponentielle. Comptes rendus, T. LXXVII, 1873.

2) Lindemann, Ueber die Zahl π. Mathem. Annalen, Bd. 20, 1882. Weierstrass, Zu Lindemann's Abhandlung „Ueber die Ludolph'sche

allmählich so völlig beseitigt sind, dass sich der Beweis jetzt mit ganz elementaren Mitteln und auf die einfachste Weise führen lässt.

Wenn wir, wie schon früher, mit $\Pi(n)$ das Product

$$\Pi(n) = 1.2.3\ldots n$$

bezeichnen, so wird, wenn x eine beliebige Grösse ist,

$$(1) \qquad \frac{x^n}{\Pi(n)}$$

mit unendlich wachsendem n sich der Grenze Null nähern, und zwar stärker, als die Glieder einer fallenden geometrischen Reihe.

Denn ist k eine ganze Zahl, die grösser ist als der absolute Werth von x, so ist der absolute Werth von $x:h$ immer dann ein echter Bruch, wenn h gleich oder grösser als k ist. Folglich ist

$$\left|\frac{x^n}{\Pi(n)}\right| = \left|\frac{x^k}{\Pi(k)}\frac{x}{k+1}\frac{x}{k+2}\cdots\frac{x}{n}\right| < \left|\frac{x^k}{\Pi(k)}\right|\left|\frac{x}{k}\right|^{n-k}.$$

Hieraus folgt, dass die unendliche Reihe

$$(2) \qquad e^x = 1 + x + \frac{x^2}{\Pi(2)} + \frac{x^3}{\Pi(3)} + \cdots$$

für alle Werthe von x convergirt, und durch sie definiren wir die Exponentialfunction e^x, deren einfachste Eigenschaften wir hier aus der Analysis voraussetzen. Insbesondere gilt für zwei beliebige Werthe x, y die Relation

$$e^{x+y} = e^x e^y,$$

aus der dann folgt, dass e^n für ein ganzes positives n die n^{te} Potenz der Zahl

$$(3) \qquad e = 2 + \frac{1}{\Pi(2)} + \frac{1}{\Pi(3)} + \frac{1}{\Pi(4)} + \cdots = 2{,}718281828459\cdots$$

ist.

Wenn nun r irgend eine ganze positive Zahl bedeutet, so können wir die Formel (2) so darstellen:

$$(4) \qquad \Pi(r)\,e^x = \Pi(r) + \frac{\Pi(r)}{\Pi(1)}x + \frac{\Pi(r)}{\Pi(2)}x^2 + \cdots + x^r + x^r\,U_r,$$

Zahl". Sitzungsbericht der Berliner Akademie, 3. December 1885. Die Arbeiten von Hilbert, Hurwitz und Gordan finden sich alle drei in Band 43 der Mathematischen Annalen (1893), die beiden ersten auch in den Göttinger Nachrichten von 1893.

worin

(5) $$U_r = \frac{x}{r+1} + \frac{x^2}{(r+1)(r+2)} + \frac{x^3}{(r+1)(r+2)(r+3)} + \cdots,$$

und diese Formel gilt auch für $r = 0$, wenn man $\Pi(0) = 1$ annimmt.

Bezeichnen wir den absoluten Werth von x mit ξ, so ist nach dem in der Einleitung bewiesenen Satze, dass der absolute Werth einer Summe niemals grösser ist als die Summe der absoluten Werthe ihrer Theile, der absolute Werth von U_r gewiss nicht grösser als

$$\frac{\xi}{r+1} + \frac{\xi^2}{(r+1)(r+2)} + \frac{\xi^3}{(r+1)(r+2)(r+3)} + \cdots,$$

also kleiner als

$$1 + \frac{\xi}{1} + \frac{\xi^2}{1.2} + \frac{\xi^3}{1.2.3} + \cdots = e^\xi.$$

Wenn wir daher

$$U_r = q_r e^\xi$$

setzen, so ist q_r eine Function von x, von der wir nur so viel feststellen, dass ihr absoluter Werth kleiner als 1 ist.

Hiernach stellen wir die Formel (4) für $r = 0, 1, \ldots, n$ auf, und schreiben die Glieder, in umgekehrter Reihenfolge geordnet, übersichtlich so:

$$\Pi(n) e^x = q_n x^n e^\xi + x^n + n x^{n-1} + n(n-1) x^{n-2} + \cdots + \Pi(n)$$

(6) $$\Pi(n-1) e^x = q_{n-1} x^{n-1} e^\xi + x^{n-1} + (n-1) x^{n-2} + (n-1)(n-2) x^{n-3} + \cdots$$

. . . .

$$e^x = q_0 e^\xi + 1.$$

Nun nehmen wir eine beliebige ganze Function n^{ten} Grades von x an:

(7) $$f(x) = c_n x^n + c_{n-1} x^{n-1} + c_{n-2} x^{n-2} + \cdots + c_0,$$

und ihre Derivirten

$$f'(x) = n c_n x^{n-1} + (n-1) c_{n-1} x^{n-2} + \cdots$$

(8) $$f''(x) = n(n-1) c_n x^{n-2} + (n-1)(n-2) c_{n-1} x^{n-3} + \cdots$$

. . . .

$$f^{(n)}(x) = \Pi(n)\, c_n,$$

und setzen noch zur Abkürzung

(9) $$F(x) = f(x) + f'(x) + f''(x) + \cdots + f^{(n)}(x).$$

Es ist dann $F(x)$ eine ganze Function von x vom Grade n. Setzen wir endlich noch

$$(10) \qquad Q(x) = c_n q_n x^n + c_{n-1} q_{n-1} x^{n-1} + \cdots + c_0 q_0,$$

$$(11) \qquad P = c_n \Pi(n) + c_{n-1} \Pi(n-1) + \cdots + c_0,$$

so ist $Q(x)$ von x abhängig, wenn auch nicht rational durch x ausdrückbar; P aber ist von x unabhängig.

Wenn wir nun die Gleichungen (6) der Reihe nach mit $c_n, c_{n-1}, \ldots, c_0$ multipliciren und addiren, so folgt

$$(12) \qquad e^x P = F(x) + e^\xi Q(x).$$

Diese Formel ist nun der Ausgangspunkt der weiteren Schlüsse.

Nehmen wir an, es sei e eine algebraische Zahl, so muss eine Gleichung, deren Grad m sei, bestehen:

$$(13) \qquad C_0 + C_1 e + C_2 e^2 + \cdots + C_m e^m = 0,$$

deren Coëfficienten $C_0, C_1, \ldots, C_m$ ganze rationale Zahlen sind, von denen C_0 und C_m von Null verschieden sind. Es handelt sich darum, die Unmöglichkeit dieser Annahme darzuthun.

Zu diesem Zwecke setzen wir in der Gleichung (12) für x der Reihe nach die ganzen Zahlen $0, 1, 2, \ldots, m$, so dass ξ mit x identisch wird, multipliciren mit $C_0, C_1, \ldots, C_m$ und addiren. Dann ergiebt sich nach (13), da P von x unabhängig ist:

$$(14) \qquad \begin{aligned} 0 = {} & C_0 F(0) + C_1 F(1) + \cdots + C_m F(m) \\ & + C_0 Q(0) + C_1 e\, Q(1) + \cdots + C_m e^m Q(m), \end{aligned}$$

und nun soll aus einer passenden Annahme über die noch willkürliche Function $f(x)$ nachgewiesen werden, dass die Gleichung (14) unmöglich ist.

Wir wählen eine Primzahl p, die grösser ist als m [1]), und setzen

$$(15) \qquad f(x) = \frac{x^{p-1}(1-x)^p (2-x)^p \ldots (m-x)^p}{\Pi(p-1)},$$

---

[1]) Dass es immer eine Primzahl p giebt, die grösser ist, als eine beliebige Zahl μ, ist schon bei Euklid bewiesen (Elemente, Buch IX. Nr. XX, Bd. 2 der Heiberg'schen Ausgabe). Der Beweis ist einfach der, dass die ganze Zahl $\Pi(\mu) + 1$, die offenbar grösser als μ ist, durch keine Primzahl theilbar ist, die nicht grösser als μ ist, weil diese Zahl bei der Theilung durch jede der Zahlen $2, 3, \ldots, \mu$ den Rest 1 ergiebt. Es ist also unmöglich, dass keine Primzahl über μ liegt.

so dass der Grad n von $f(x)$ gleich $(m+1)p-1$ ist, und wir beweisen nun zweierlei:

1) $C_0 F(0) + C_1 F(1) + \cdots + C_m F(m)$ ist eine von Null verschiedene ganze Zahl, also, vom Zeichen abgesehen, mindestens gleich 1,

2) $C_0 Q(0) + C_1 e Q(1) + \cdots + C_m e^m Q(m)$ ist kleiner als 1,

beides unter der Voraussetzung, dass über p passend verfügt wird. Ist dies beides bewiesen, so erkennt man die Unmöglichkeit der Gleichung (14) und also die der Gleichung (13), aus der (14) gefolgert war.

Ordnen wir den Zähler von $f(x)$ nach Potenzen von x, so ergiebt sich ein Ausdruck der Form:

$$(16) \qquad f(x) = \frac{A_{p-1} x^{p-1} + A_p x^p + A_{p+1} x^{p+1} + \cdots}{\Pi(p-1)},$$

worin $A_{p-1}, A_p, A_{p+1}, \ldots$ ganze Zahlen sind, und $A_{p-1} = [\Pi(m)]^p$, also gewiss nicht durch p theilbar. Es ist daher, wenn man (16) mit der Taylor'schen Entwickelung

$$f(x) = f(0) + x f'(0) + \frac{x^2}{\Pi(2)} f''(0) + \cdots$$

vergleicht,

$$f(0) = f'(0) = f''(0) = \cdots = f^{(p-2)}(0) = 0,$$

$$f^{(p-1)}(0) = A_{p-1}, \; f^{(p)}(0) = p A_p, \; f^{(p+1)}(0) = p(p+1) A_{p+1} \ldots,$$

also

$$F(0) = A_{p-1} + p A_{p+1} + p(p+1) A_{p+1} + \cdots,$$

eine durch p nicht theilbare ganze Zahl. Ordnen wir aber $f(x)$ nach Potenzen von $x-1$, so folgt:

$$f(x) = \frac{B_p (x-1)^p + B_{p+1} (x-1)^{p+1} + \cdots}{\Pi(p-1)},$$

worin die $B_p, B_{p+1}, \ldots$ wieder ganze Zahlen sind. Daraus folgt, wie oben, durch Vergleichung mit

$$f(x) = f(1) + (x-1) f'(1) + \frac{(x-1)^2}{\Pi(2)} f''(1) + \cdots$$

$$F(1) = p B_p + p(p+1) B_{p+1} + \cdots,$$

folglich ist $F(1)$ eine durch p theilbare ganze Zahl, und genau auf demselben Wege ergiebt sich, dass $F(2), F(3), \ldots, F(m)$ durch p theilbare ganze Zahlen sind. Da man nun auch p so gross wählen kann, dass C_0 nicht durch p theilbar ist, so folgt

dass $C_0 F(0) + C_1 F(1) + \cdots + C_m F(m)$ eine nicht durch p theilbare, also auch nicht verschwindende ganze Zahl ist, und damit ist 1) bewiesen.

Wenn wir nun noch nachweisen können, dass $Q(x)$ für jedes positive x durch Vergrösserung von p beliebig klein gemacht werden kann, so folgt, dass bei hinlänglich grossem p der Ausdruck 2) gewiss kleiner als 1 ist, und unser Beweis ist vollendet.

Gehen wir aber zu dem Ausdrucke (10) für $Q(x)$ zurück und bezeichnen mit $\gamma_n, \gamma_{n-1}, \ldots, \gamma_0$ die absoluten Werthe der Coëfficienten $c_n, c_{n-1}, \ldots, c_0$ von $f(x)$, so sehen wir, da die $q_n, q_{n-1}, \ldots$ dem absoluten Werthe nach kleiner als 1 sind, dass für jedes positive x der absolute Werth von $Q(x)$ kleiner ist als

(17) $$\psi(x) = \gamma_n x^n + \gamma_{n-1} x^{n-1} + \cdots + \gamma_0.$$

Die Coëfficienten $c_n, c_{n-1}, \ldots, c_0$ der Function $f(x)$ in (15) unterscheiden sich aber von den $\gamma_n, \gamma_{n-1}, \ldots, \gamma_0$ nur durch das Vorzeichen. Ersetzen wir daher x durch $-x$, bilden also die Function

$$f(-x) = \frac{x^{p-1}(1+x)^p (2+x)^p \ldots (m+x)^p}{\Pi(p-1)},$$

so hat diese Function dieselben Coëfficienten, wie $f(x)$, aber alle mit positiven Vorzeichen. Sie ist also keine andere, als die Function $\psi(x)$.

Setzen wir also noch

$$X = x(1+x)(2+x)\ldots(m+x),$$

so wird

(18) $$\psi(x) = \frac{X}{x} \cdot \frac{X^{p-1}}{\Pi(p-1)},$$

und dies nähert sich, wie am Anfange dieses Paragraphen nachgewiesen ist, mit unendlich wachsendem p der Grenze Null.

Es ist also e eine transcendente Zahl.

§. 206.

Transcendenz der Zahl π.

Mit denselben Hülfsmitteln lässt sich nun auch die Transcendenz der Zahl π beweisen. Als Definition dieser Zahl dient uns dabei, dass es die kleinste positive Zahl ist, die der Gleichung

(1) $$e^{i\pi} = -1$$

genügt, wenn e^x durch die Formel §. 205, (2) definirt wird.

Nehmen wir also an, es sei π und folglich auch $i\pi$ eine algebraische Zahl, so ist $i\pi$ eine der Wurzeln einer irreduciblen rationalen Gleichung $\chi(x) = 0$, deren Coëfficienten ganze rationale Zahlen sind.

Bezeichnen wir die sämmtlichen Wurzeln dieser algebraischen Gleichung mit $\beta_1, \beta_2, \ldots, \beta_\nu$, und bezeichnen den Coëfficienten von x^ν in χ mit a, so ist

(2) $$\chi(x) = a(x-\beta_1)(x-\beta_2)\ldots(x-\beta_\nu),$$

und die Producte $a\beta_1, a\beta_2, \ldots, a\beta_\nu$ sind **ganze** algebraische Zahlen, ihre ganzen symmetrischen Functionen also **ganze rationale Zahlen** (§. 133).

Da nun die Zahl $i\pi$ unter den β vorkommen soll, so ist nach (1):

$$(1+e^{\beta_1})(1+e^{\beta_2})\ldots(1+e^{\beta_\nu}) = 0,$$

und wenn wir die Multiplication ausführen, so ergiebt sich eine Gleichung:

$$1 + \Sigma\, e^{\beta_i} + \Sigma\, e^{\beta_i+\beta_h} + \Sigma\, e^{\beta_i+\beta_h+\beta_k} + \cdots = 0.$$

Unter den Exponenten in dieser Summe kann mehrmals die Zahl Null vorkommen; wir wollen annehmen $(C-1)$ mal, so dass C eine positive ganze Zahl, mindestens $= 1$, ist. Die übrigen Exponenten β_i, $\beta_i + \beta_h$, $\beta_i + \beta_h + \beta_k, \ldots$, die zum Theil auch unter einander gleich sein können, wollen wir mit $\alpha_1, \alpha_2, \ldots, \alpha_\mu$ bezeichnen, so dass die Gleichung besteht:

(3) $$C + e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_\mu} = 0.$$

Hierin sind nun die $\alpha_1, \alpha_2, \ldots, \alpha_\mu$ algebraische Zahlen, die, mit der ganzen rationalen Zahl a multiplicirt, in ganze algebraische Zahlen übergehen.

Die symmetrischen Functionen der sämmtlichen Summen β_i, $\beta_i + \beta_h$, $\beta_i + \beta_h + \beta_k, \ldots$ sind aber zugleich symmetrische Functionen der $\beta_1, \ldots, \beta_\nu$, und folglich rationale Zahlen. Diese Summen sind folglich auch die Wurzeln einer rationalen Gleichung, und da man die Wurzel 0, so oft sie vorhanden ist, absondern kann, so sind auch die $\alpha_1, \alpha_2, \ldots, \alpha_\mu$ die Wurzeln einer rationalen Gleichung; die symmetrischen Grundfunctionen der $a\alpha_1, a\alpha_2, \ldots, a\alpha_\mu$ sind **ganze rationale Zahlen**.

Die absoluten Werthe der Zahlen

$$\alpha_1, \alpha_2, \ldots, \alpha_\mu$$

sollen jetzt mit

$$a_1, a_2, \ldots, a_\mu$$

bezeichnet werden.

Wenn wir nun in der Gleichung (12) des vorigen Paragraphen $x = 0, \alpha_1, \alpha_2, \ldots, \alpha_\mu$ setzen und die Gleichung (3) anwenden, so ergiebt sich:

$$(4)\quad \begin{aligned} 0 = {} & C F(0) + F(\alpha_1) + F(\alpha_2) + \cdots + F(\alpha_\mu) \\ & + C Q(0) + e^{\alpha_1} Q(\alpha_1) + e^{\alpha_2} Q(\alpha_2) + \cdots + e^{\alpha_\mu} Q(\alpha_\mu), \end{aligned}$$

und wir haben die Unmöglichkeit einer solchen Gleichung bei einer geeigneten Wahl von $f(x)$ darzuthun.

Es sei wieder p eine zu unbegrenztem Wachsen bestimmte Primzahl, und

$$(5)\quad f(x) = \frac{a^{\mu p + p - 1} x^{p-1} (x - \alpha_1)^p (x - \alpha_2)^p \ldots (x - \alpha_\mu)^p}{\Pi(p-1)},$$

so dass $f(x)$ eine Function mit rationalen Coëfficienten ist.

Wir bilden nun, wie im vorigen Paragraphen, durch Ordnen nach Potenzen von x:

$$f(x) = \frac{A_{p-1} x^{p-1} + A_p x^p + A_{p+1} x^{p+1} \ldots}{\Pi(p-1)},$$

worin die $A_{p-1}, A_p, \ldots$ ganze rationale Zahlen sind, und

$$A_{p-1} = (-1)^\mu a^{\mu p + p - 1} \alpha_1^p \alpha_2^p \ldots \alpha_\mu^p.$$

Wenn wir also p grösser als jede der ganzen Zahlen

$$a,\ a^\mu \alpha_1 \alpha_2 \ldots \alpha_\mu$$

annehmen, so ist A_{p-1} durch p nicht theilbar, und es wird

$$F(0) = A_{p-1} + p A_p + p(p+1) A_{p+1} + \cdots,$$

d. h. eine durch p nicht theilbare ganze Zahl. Ebenso ist, wenn p gross genug genommen wird, C durch p nicht theilbar.

Andererseits ordnen wir den Zähler von $f(x)$ nach Potenzen von $a(x - \alpha_1)$ und erhalten

$$f(x) = \frac{B_p a^p (x - \alpha_1)^p + B_{p+1} a^{p+1} (x - \alpha_1)^{p+1} + \cdots}{\Pi(p-1)},$$

worin die $B_p, B_{p+1}, \ldots$ zwar nicht mehr rationale, wohl aber g a n z e a l g e b r a i s c h e Z a h l e n sind, da der Zähler von $f(x)$ eine ganzzahlige Function von $a x, a\alpha_1, \ldots, a\alpha_\mu$ ist.

Hieraus folgt nun, wie im vorigen Paragraphen:

$$F(\alpha_1) = p B_p a^p + p(p+1) B_{p+1} a^{p+1} + \cdots$$

Bildet man auf die gleiche Weise $F(\alpha_2), \ldots, F(\alpha_\mu)$, und beachtet, dass die Summe $B_p(\alpha_1) + B_p(\alpha_2) + \cdots + B_p(\alpha_\mu)$ eine ganze rationale Zahl ist, so folgt, dass

$$F(\alpha_1) + F(\alpha_2) + \cdots + F(\alpha_\mu)$$

eine durch p theilbare ganze rationale Zahl ist. Daraus ergiebt sich endlich, dass

$$CF(0) + F(\alpha_1) + F(\alpha_2) + \cdots + F(\alpha_\mu)$$

eine nicht durch p theilbare, also auch nicht verschwindende, ganze rationale Zahl ist, die daher, vom Vorzeichen abgesehen, mindestens $= 1$ ist.

Können wir nun endlich noch beweisen, dass auch bei der jetzigen Annahme über f die Function $Q(x)$ für jedes endliche x bei hinlänglicher Vergrösserung von p beliebig klein gemacht werden kann, so ergiebt sich, genau wie oben, die Unmöglichkeit der Gleichung (4).

Dies lässt sich aber folgendermaassen einsehen: Wir betrachten statt der Function

$$(6) \qquad f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$$

die Function

$$\psi(x) = \frac{a^{\mu p + p - 1}\, x^{p-1}\, (x + a_1)^p\, (x + a_2)^p \ldots (x + a_\mu)^p}{\Pi(p-1)}$$

$$= \gamma_n x^n + \gamma_{n-1} x^{n-1} + \cdots + \gamma_0,$$

die nun lauter positive (aber nicht nothwendig rationale) Coëfficienten hat. Die Coëfficienten $c_n, c_{n-1} \ldots$ sind durch Multiplication und Addition aus den Zahlen $a, -\alpha_1, -\alpha_2, \ldots, -\alpha_\mu$ gebildet, und die entsprechenden Coëfficienten $\gamma_n, \gamma_{n-1} \ldots$ erhält man daraus, wenn man die $-\alpha_1, -\alpha_2, \ldots, -\alpha_\mu$ durch ihre absoluten Werthe $a_1, a_2, \ldots, a_\mu$ ersetzt, woraus nach dem schon oben erwähnten Satze der Einleitung folgt, dass die Coëfficienten $\gamma_n, \gamma_{n-1}, \ldots$ gewiss nicht kleiner sind, als die absoluten Werthe der entsprechenden $c_n, c_{n-1} \ldots$

Nun ist für jedes endliche x, dessen absoluter Werth ξ ist, der absolute Werth von $Q(x)$ nach §. 205, (10) kleiner, oder wenigstens nicht grösser als

$$\gamma_n \xi^n + \gamma_{n-1} \xi^{n-1} + \cdots + \gamma_0 = \psi(\xi),$$

und dass $\psi(\xi)$ unter jede Grenze heruntersinkt, wenn p gross genug wird, schliesst man aus der Darstellung:

$$\psi(x) = \frac{X}{a x} \frac{X^{p-1}}{\Pi(p-1)},$$

wenn

$$X = a^{\mu+1}\, x\, (x + a_1)\, (x + a_2) \ldots (x + a_\mu)$$

gesetzt ist.

Damit ist bewiesen:

Die Zahl π ist eine transcendente Zahl. Die „Quadratur des Kreises“ kann nicht durch geometrische Construction, bei der nur algebraische Curven und Flächen angewandt werden, gelöst werden.

§. 207.

Der allgemeine Satz von Lindemann über die Exponentialfunction.

Die Transcendenz der Zahlen e und π, die hierdurch bewiesen ist, ist als specieller Fall in einem sehr allgemeinen Theoreme über die Exponentialfunction enthalten, das **Lindemann** in der oben erwähnten Abhandlung angekündigt hat, von dem ein ausgeführter Beweis in der citirten Abhandlung von **Weierstrass** enthalten ist. Wir wollen diesen Satz hier zum Schluss noch beweisen mit Anwendung derselben Hülfsmittel, die wir für die beiden speciellen Fälle benutzt haben. Der Satz lautet so:

I. Es besteht keine Gleichung von der Form

$$C_1 e^{z_1} + C_2 e^{z_2} + \cdots + C_m e^{z_m} = 0, \tag{1}$$

in der die Coëfficienten $C_1, C_2, \ldots, C_m$ algebraische Zahlen und die Exponenten $z_1, z_2, \ldots, z_m$ von einander verschiedene algebraische Zahlen sind, es sei denn, dass alle Coëfficienten $C_1, C_2, \ldots, C_m$ gleich Null sind.

Um ihn zu beweisen, leiten wir zunächst einen Hülfssatz ab:

Es seien

$$\alpha_1, \alpha_2, \ldots, \alpha_r$$

beliebige reelle oder imaginäre, jedoch von einander verschiedene Grössen, und

$$A_1, A_2, \ldots, A_r$$

ebenfalls beliebige Grössen, die nicht alle verschwinden.

Dasselbe soll von den zwei Grössenreihen

$$\beta_1, \beta_2, \ldots, \beta_s$$
$$B_1, B_2, \ldots, B_s$$

gelten. Wir bezeichnen mit

$$\gamma_1, \gamma_2, \ldots, \gamma_t$$

die von einander verschiedenen unter den rs Summen $\alpha_i + \beta_k$, und setzen

$$(2)\qquad \begin{aligned} A &= A_1 e^{\alpha_1} + A_2 e^{\alpha_2} + \cdots + A_r e^{\alpha_r} \\ B &= B_1 e^{\beta_1} + B_2 e^{\beta_2} + \cdots + B_s e^{\beta_s}, \end{aligned}$$

$$(3)\qquad A\,B = C_1 e^{\gamma_1} + C_2 e^{\gamma_2} + \cdots + C_t e^{\gamma_t}.$$

Der zu beweisende Hülfssatz lautet dann:

1. Die Coëfficienten $C_1, C_2, \ldots, C_t$ können nicht alle verschwinden.

Beim Beweise dieses Satzes können wir offenbar annehmen, dass von den Coëfficienten $A_1, A_2, \ldots, A_r, B_1, B_2, \ldots, B_s$ keiner verschwindet (da wir die etwa verschwindenden einfach weglassen können).

Des kürzeren Ausdrucks wegen nennen wir für den Augenblick, wenn a, b zwei verschiedene complexe Zahlen sind, a kleiner als b, $(a < b)$, wenn der reelle Theil von a kleiner ist als der reelle Theil von b, oder wenn die reellen Theile gleich und der imaginäre Theil von a kleiner ist, als der imaginäre Theil von b.

Ist dann in diesem Sinne $a < b$, $b < c$, so ist auch $a < c$, und ist $a < b$, $c < d$, so ist $a + c < b + d$.

Unter jeder endlichen Reihe von einander verschiedener complexer Zahlen giebt es dann eine bestimmte kleinste, und wenn also α_1 die kleinste unter den Zahlen α, β_1 die kleinste unter den Zahlen β ist, so ist $\alpha_1 + \beta_1$ die kleinste unter den Zahlen γ, und diese Summe ist keiner der anderen Summen $\alpha_i + \beta_k$ gleich. Es ist also $C_1 = A_1 B_1$ und C_1 von Null verschieden, w. z. b. w.

Dieser Satz lässt sich nun durch vollständige Induction sofort verallgemeinern.

2. Sind
$$\begin{aligned} A' &= A_1' e^{\alpha_1'} + A_2' e^{\alpha_2'} + \cdots \\ A'' &= A_1'' e^{\alpha_1''} + A_2'' e^{\alpha_2''} + \cdots \\ A''' &= A_1''' e^{\alpha_1'''} + A_2''' e^{\alpha_2'''} + \cdots \\ &\cdots\cdots\cdots\cdots \end{aligned}$$
Summen von der Form (2) in beliebiger Anzahl, und $\gamma_1, \gamma_2, \ldots$ die von einander verschiedenen unter den Summen $\alpha_h' + \alpha_i'' + \alpha_k''' + \cdots$, so sind in dem Producte
$$(4)\qquad A' A'' A''' \cdots = C_1 e^{\gamma_1} + C_2 e^{\gamma_2} + \cdots$$
nicht alle Coëfficienten $C_1, C_2, \ldots$ gleich Null.

Dieser Hülfssatz gestattet uns zunächst, beim Beweise des Theorems (1) die vereinfachende Voraussetzung zu machen, die Coëfficienten $C_1, C_2, \ldots, C_m$ seien ganze rationale Zahlen.

Angenommen nämlich, es bestehe eine Gleichung

$$(5) \qquad X_1 e^{x_1} + X_2 e^{x_2} + \cdots = 0$$

mit algebraischen Coëfficienten $X_1, X_2, \ldots$ und von einander verschiedenen Exponenten $x_1, x_2, \ldots$, so können wir immer annehmen, die $X_1, X_2, \ldots$ gehören einem und demselben algebraischen Körper Ω an.

Wir bezeichnen mit $u_1, u_2, \ldots$ Variable und bilden die Norm der Linearform $X_1 u_1 + X_2 u_2 + \cdots$

$$(6) \qquad N(X_1 u_1 + X_2 u_2 + \cdots) = \Phi(u_1, u_2, \ldots),$$

die eine ganze homogene Function der Variablen u mit rationalen Coëfficienten ist, deren Grad gleich dem Grade des Körpers Ω ist. Setzen wir in (6)

$$u_1 = e^{x_1}, \; u_2 = e^{x_2}, \ldots,$$

so geht jedes Product von Variablen u in eine Grösse von der Form e^z über, worin z eine Summe von Zahlen x ist, und $\Phi(u_1, u_2, \ldots)$ wird ein Ausdruck von der Form $C_1 e^{z_1} + C_2 e^{z_2} + \cdots$, dessen Coëfficienten rationale Zahlen sind, die, wenn die $X_1, X_2, \ldots$ nicht alle verschwinden, nach 2. auch dann nicht alle Null sein können, wenn die unter einander gleichen unter den Gliedern der Function $\Phi(e^{x_1}, e^{x_2}, \ldots)$ in ein einziges Glied Ce^z zusammengefasst werden. Wenn nun aber die Gleichung (5) besteht, so ist auch $\Phi(e^{x_1}, e^{x_2}, \ldots) = 0$, und folglich

$$C_1 e^{z_1} + C_2 e^{z_2} + \cdots = 0.$$

Sind unter den $C_1, C_2, \ldots$ gebrochene Zahlen, so können wir sie durch Multiplication der ganzen Gleichung mit dem Hauptnenner in ganze Zahlen verwandeln.

3. Es braucht also jetzt nur noch bewiesen zu werden, dass die Gleichung (1) für kein System ganzer rationaler Zahlen $C_1, C_2, \ldots, C_m$, die nicht alle verschwinden, bestehen kann.

Demnach nehmen wir jetzt an, es bestehe eine Gleichung

$$(7) \qquad A_1 e^{x_1} + A_2 e^{x_2} + \cdots = 0,$$

deren Coëfficienten $A_1, A_2, \ldots$ ganze rationale Zahlen sind,

die nicht alle $= 0$ sind, worin die Exponenten $x_1, x_2, \ldots$ von einander verschiedene algebraische Zahlen sind. Wir bezeichnen mit Ω einen Normalkörper, dem alle diese Zahlen $x_1, x_2, \ldots$ angehören, und mit Θ eine primitive Zahl dieses Körpers, ferner mit

$$\sigma' = (\Theta, \Theta'),\ \sigma'' = (\Theta, \Theta''), \ldots$$

die Substitutionen des Körpers Ω. Wenn durch eine dieser Substitutionen, σ', die Zahlen $x_1, x_2, \ldots$ in $x_1', x_2', \ldots$ übergehen, so müssen auch diese von einander verschieden sein.

Es sei jetzt u eine Variable und

$$(8) \qquad U = A_1 e^{u x_1} + A_2 e^{u x_2} + \cdots$$

Hierin machen wir die sämmtlichen Substitutionen $\sigma', \sigma'', \ldots$ und bezeichnen die so entstehenden Functionen mit $U', U'', \ldots$ Das Product aller dieser Functionen können wir, obwohl es sich nicht bloss um algebraische Zahlen handelt, die Norm von U nennen. Dieses Product hat die Form

$$(9) \qquad N(U) = C_1 e^{u z_1} + C_2 e^{u z_2} + \cdots,$$

worin die $C_1, C_2, \ldots$ gleichfalls ganze rationale Zahlen sind. Die $z_1, z_2, \ldots$ sind Zahlen des Körpers Ω, die wir, wenn wir die Glieder mit gleichen Exponenten in ein einziges Glied zusammenfassen, als von einander verschieden voraussetzen dürfen. Zugleich ist wegen (7)

$$(10) \qquad C_1 e^{z_1} + C_2 e^{z_2} + \cdots = 0.$$

Der Ausdruck auf der rechten Seite von (9) hat aber noch, wie seine Entstehung als Norm zeigt, die Eigenschaft, ungeändert zu bleiben, wenn irgend eine der Substitutionen $\sigma', \sigma'', \ldots$ gemacht wird. Entwickelt man aber (9) nach Potenzen von u, so muss diese Unveränderlichkeit von jedem Gliede dieser Reihenentwickelung gelten, also wenn h ein beliebiger ganzer positiver Exponent ist, für

$$C_1 z_1^h + C_2 z_2^h + \cdots;$$

diese Summe ist aber eine Zahl des Körpers Ω, und daher eine rationale Zahl. Dies können wir dahin zusammenfassen:

Bedeutet $g(z)$ irgend eine ganze Function von z mit rationalen Coëfficienten, so ist

$$C_1 g(z_1) + C_2 g(z_2) + \cdots$$

eine rationale Zahl.

4. **Der Beweis des Theorems I. ist hierdurch auf den Beweis des folgenden speciellen Falles zurückgeführt: Besteht eine Gleichung**

(11) $$C_1 e^{z_1} + C_2 e^{z_2} + \cdots + C_m e^{z_m} = 0,$$

in der die $z_1, z_2, \ldots, z_m$ von einander verschiedene algebraische Zahlen sind, in der $C_1, C_2, \ldots, C_m$ und die Verbindungen

(12) $$C_1\, g(z_1) + C_2\, g(z_2) + \cdots + C_m\, g(z_m)$$

rationale Zahlen sind, wenn $g(z)$ irgend eine ganze Function mit rationalen Coëfficienten ist, so müssen die $C_1, C_2, \ldots, C_m$ alle verschwinden.

Um diesen Satz zu beweisen, bestimmen wir zunächst eine positive ganze rationale Zahl c so, dass

(13) $$x_1 = c z_1,\; x_2 = c z_2, \ldots, x_m = c z_m$$

ganze algebraische Zahlen werden (§. 133, 5.). Wir nehmen die Coëfficienten $C_1, C_2, \ldots, C_m$ als ganze rationale Zahlen an, und bilden eine ganze Function

(14) $$\varphi(x) = a x^r + a_1 x^{r-1} + \cdots + a_r$$

mit ganzen rationalen Zahlencoëfficienten, die folgende Eigenschaften hat:

1) Die Zahlen $x_1, x_2, \ldots, x_m$ kommen unter den Wurzeln von $\varphi(x) = 0$ vor.

2) Die Summe

$$C_1\, \varphi'(x_1) + C_2\, \varphi'(x_2) + \cdots + C_m\, \varphi'(x_m) = k,$$

die nach den Voraussetzungen (12), (13) eine ganze rationale Zahl ist, ist von Null verschieden.

Um einzusehen, dass eine solche Function $\varphi(x)$ immer existirt, nehme man zunächst eine Function $\chi(x)$, die nur der Bedingung 1) genügt, und der zweiten, dass keine der Zahlen $x_1, x_2, \ldots, x_m$ eine Doppelwurzel von $\chi(x)$ ist, eine solche Function existirt offenbar [man kann z. B., um eine Function χ zu bilden, die Norm des Productes $(x - x_1)\,(x - x_2)\ldots(x - x_m)$ von gemeinsamen Theilern mit ihren Derivirten befreien]. Setzt man dann

$$\varphi(x) = x^h \chi(x),\; \varphi'(x_1) = x_1^h \chi'(x_1),\; \varphi'(x_2) = x_2^h \chi'(x_2) \ldots,$$

so kann die Summe

$$C_1 \varphi'(x_1) + \cdots + C_m \varphi'(x_m) = C_1 \chi'(x_1) x_1^h + \cdots + C_m \chi'(x_m) x_m^h$$

gewiss nicht für jeden Exponenten h verschwinden, da sonst gegen die Voraussetzung $C_1 \chi'(x_1) \ldots C_m \chi'(x_m)$ alle gleich Null sein müssten.

Nachdem so die Existenz einer Function $\varphi(x)$, wie sie verlangt war, festgestellt ist, wenden wir die Formel §. 205, (12) an:

$$e^x P(x) = F(x) + e^\xi Q(x).$$

Wir setzen darin $x = z_1, z_2, \ldots, z_m$, und bezeichnen die absoluten Werthe von $z_1, z_2, \ldots, z_m$ mit $\xi_1, \xi_2, \ldots, \xi_m$.

Dann ergiebt sich nach (11):

$$(15) \quad \begin{aligned} 0 = & C_1 F(z_1) + C_2 F(z_2) + \cdots + C_m F(z_m) \\ & + C_1 e^{\xi_1} Q(z_1) + C_2 e^{\xi_2} Q(z_2) + \cdots + C_m e^{\xi_m} Q(z_m), \end{aligned}$$

und es ist, wenn $f(x)$ eine beliebige ganze Function n^{ten} Grades ist

$$(16) \qquad F(z) = f(z) + f'(z) + \cdots + f^{(n)}(z).$$

Wir setzen, indem wir mit p eine natürliche Primzahl bezeichnen, die beliebig gross genommen werden kann, $x = cz$ [nach (13)] und

$$(17) \qquad f(z) = \frac{\varphi(x)^{p-1} \varphi'(x)}{\Pi(p-1)},$$

wenn $\varphi(x)$ die den Bedingungen 1), 2) genügende Function ist.

Durch Ordnen nach Potenzen von $(x - x_1)$ mag sich ergeben:

$$\begin{aligned} \varphi(x)^{p-1} \varphi'(x) = & \varphi'(x_1)^p (x - x_1)^{p-1} + A_p(x_1)(x - x_1)^p \\ & + A_{p+1}(x_1)(x - x_1)^{p+1} + \cdots, \end{aligned}$$

und darin sind die $A_p(x_1), A_{p+1}(x_1), \ldots$ ganze algebraische Zahlen, und zwar rationale Functionen von x_1. Andererseits ist nach dem Taylor'schen Lehrsatze:

$$f(z) = f(z_1) + (z - z_1) f'(z_1) + \frac{(z - z_1)^2}{1.2} f''(z_1) + \cdots$$

und $c(z - z_1) = x - x_1$. Die Vergleichung ergiebt alsdann

$$\begin{aligned} & f(z_1) = 0, f'(z_1) = 0, \ldots, f^{(p-2)}(z_1) = 0, f^{(p-1)}(z_1) = c^{p-1} \varphi'(x_1)^p, \\ & f^{(p)}(z_1) = p c^p A_p(x_1), f^{(p+1)}(z_1) = p(p+1) c^{p+1} A_{p+1}(x_1), \ldots, \end{aligned}$$

und folglich

$$F(z_1) = c^{p-1} \varphi'(x_1)^p + p c^p A_p(x_1) + p(p+1) c^{p+1} A_{p+1}(x_1) + \cdots;$$

hierin kann x_1, z_1 durch x_2, z_2 oder durch x_3, z_3 u. s. f. ersetzt werden.

Danach ist die ganze rationale Zahl

$$C_1 F(z_1) + C_2 F(z_2) + \cdots + C_m F(z_m)$$

nach dem Modul p mit

$$c^{p-1} [C_1 \varphi'(x_1)^p + C_2 \varphi'(x_2)^p + \cdots + C_m \varphi'(x_m)^p]$$

congruent. Da nun $C_1, C_2, \ldots, C_p$ ganze rationale Zahlen sind, so ist $C_1^p \equiv C_1$, $C_2^p \equiv C_2, \ldots \pmod{p}$, und es ergiebt sich durch Anwendung des polynomischen Lehrsatzes:

$$C_1 \varphi'(x_1)^p + C_2 \varphi'(x_2)^p + \cdots + C_m \varphi'(x_m)^p \equiv$$
$$[C_1 \varphi'(x_1) + C_2 \varphi'(x_2) + \cdots + C_m \varphi'(x_m)]^p \equiv k^p \pmod{p}.$$

Danach erhalten wir also die Congruenz

$$(18) \quad C_1 F(z_1) + C_2 F(z_2) + \cdots + C_m F(z_m) \equiv c^{p-1} k^p \pmod{p}.$$

Nun sind die Zahlen c, k von p unabhängig, und wir können daher p so gross annehmen, dass es nicht in c und in k aufgeht.

5. Dann ist die Summe $C_1 F(z_1) + C_2 F(z_2) + \cdots + C_m F(z_m)$ eine von Null verschiedene ganze rationale Zahl, also dem absoluten Werthe nach mindestens gleich 1.

Wir bezeichnen nun mit $\varphi_1(x)$ die ganze Function, die sich aus $\varphi(x)$ ergiebt, wenn die negativen unter den Coëfficienten $a, a_1, a_2, \ldots$ durch ihre positiven Werthe ersetzt werden. Die Function

$$f_1(z) = \frac{\varphi_1(x)^{p-1} \varphi_1'(x)}{\Pi(p-1)},$$

die sich nach (17) ergiebt, hat dann nur positive Coëfficienten, und diese Coëfficienten sind dem absoluten Werthe nach gewiss nicht kleiner, als die entsprechenden Coëfficienten von $f(z)$, weil die Coëfficienten von $f_1(z)$ aus denselben Zahlen durch Addition entstehen, die bei der Bildung der Coëfficienten von $f(z)$ theils addirt, theils subtrahirt werden.

Hieraus aber ergiebt sich nach der Formel §. 205, (10), wenn wir mit ξ den absoluten Werth von x bezeichnen, für den absoluten Werth von $Q(z)$:

$$|Q(z)| \leqq \frac{\varphi_1(\xi)^{p-1} \varphi_1'(\xi)}{\Pi(p-1)},$$

6. und es kann also $Q(z)$ für jedes endliche z durch hinlängliche Vergrösserung von p beliebig klein gemacht werden.

Durch 5. und 6. ist aber nachgewiesen, dass, wenn p gross genug ist, die Gleichung (15) nicht bestehen kann. Dadurch ist 4. und damit das ganze Theorem I. bewiesen.

Dieser Satz gestattet nun mannigfaltige Anwendungen. Er giebt uns zunächst die Transcendenz von e, wenn wir $C_1, C_2, \ldots, z_1, z_2, \ldots$ als ganze rationale Zahlen annehmen. Er giebt ferner die Transcendenz von π. Denn aus der Gleichung $1 + e^{i\pi} = 0$ folgt nach I., dass $i\pi$ und folglich auch π nicht algebraisch sein kann.

Es folgt ferner daraus:

Für jede algebraische Zahl x, mit Ausnahme von $x = 0$, ist $X = e^x$ eine transcendente Zahl.

Für jedes algebraische X, mit Ausnahme von $X = 1$, ist jeder natürliche Logarithmus $x = \log X$ eine transcendente Zahl.

Für jeden Bogen, der zum Radius in einem algebraisch ausdrückbaren Verhältnisse x steht, mit Ausnahme von $x = 0$, ist $X = \sin x$ eine transcendente Zahl.

Dies folgt nach I. aus $2iX = e^{ix} - e^{-ix}$.

Dasselbe gilt für die anderen trigonometrischen Linien, $\cos x$, $\operatorname{tg} x$ und für die Sehne $\frac{1}{2} \sin \frac{x}{2}$. Um noch eins anzuführen: Die transcendente Gleichung $\operatorname{tg} x = \alpha x$ hat für ein algebraisches α ausser 0 nur transcendente Zahlen zu Wurzeln.

Nachträge.

I.

Irreducibilität der Kreistheilungsgleichung.

Der §. 134 des ersten Bandes bedarf in seinem letzten Theile, der von der Irreducibilität der Kreistheilungsgleichung in dem allgemeinen Falle handelt, in dem der Grad der Einheitswurzel eine aus mehreren verschiedenen Primzahlen zusammengesetzte Zahl ist, einer Berichtigung, die hier nachgetragen werden soll, und wir bitten den Leser, die genannte Stelle nach dem, was hier ausgeführt wird, zu ergänzen.

Wenn $n = ab$ gesetzt wird, a und b relativ prim sind, und ϱ, α, β primitive n^{te}, a^{te}, b^{te} Einheitswurzeln sind, so ist $\varrho = \alpha\beta$, und es ist an der angeführten Stelle bewiesen, dass, wenn ϱ Wurzel einer rationalen Gleichung $\Phi(x) = 0$ ist, unter den Wurzeln dieser Gleichung $\varrho = \alpha\beta$ alle primitiven a^{ten} Einheitswurzeln α und alle primitiven b^{ten} Einheitswurzeln β vorkommen müssen. Daraus folgt aber nicht, wie dort irrthümlich angenommen ist, dass darunter alle primitiven n^{ten} Einheitswurzeln vorkommen, weil nicht gezeigt ist, dass jedes α mit jedem β combinirt vorkommt.

Zur Ausfüllung dieser Lücke möge hier zunächst ein ganz elementarer Beweis Platz finden [1]).

Ist p eine Primzahl, so sind alle Binomialcoëfficienten für die p^{te} Potenz

$$B_h^{(p)} = \frac{p(p-1)\ldots(p-h+1)}{1.2\ldots h},$$

mit Ausnahme von $B_0^{(p)}$ und $B_p^{(p)}$, durch p theilbare ganze Zahlen,

---

[1]) Arndt, Crelle's Journ., Bd. 56, S. 178 (1859). Lebesgue, Liouville's Journ., 2. Ser., Bd. 4, S. 105 (1859).

und folglich ist, wenn u, v unbestimmte Grössen sind und die Congruenz nur auf die Coëfficienten bezogen wird,

$$(u + v)^p \equiv u^p + v^p \pmod{p}.$$

Ersetzen wir darin v wieder durch eine Summe $v + w + \cdots$, so erhalten wir durch vollständige Induction (oder auch aus dem polynomischen Lehrsatze):

$$(u + v + w + \cdots)^p \equiv u^p + v^p + w^p + \cdots \pmod{p},$$

und wenn wir diese Formel wiederholt anwenden, und unter k einen beliebigen positiven Exponenten verstehen,

$$(1) \quad (u + v + w + \cdots)^{p^k} \equiv u^{p^k} + v^{p^k} + w^{p^k} + \cdots \pmod{p}.$$

Es sei jetzt x eine Variable, $a_1, a_2, \ldots, a_\nu$ ganze rationale Zahlen,

$$f(x) = x^\nu + a_1 x^{\nu-1} + a_2 x^{\nu-2} + \cdots + a_\nu$$

eine ganze Function von x, deren Wurzeln $\alpha, \beta, \gamma, \ldots$ sein mögen, so dass

$$-a_1 = \Sigma\alpha, \quad a_2 = \Sigma\alpha\beta, \quad -a_3 = \Sigma\alpha\beta\gamma \ldots$$

die symmetrischen Grundfunctionen der $\alpha, \beta, \gamma, \ldots$ sind.

Wir bilden die Function

$$F(x) = x^\nu + A_1 x^{\nu-1} + A_2 x^{\nu-2} + \cdots + A_\nu,$$

deren Wurzeln die $p^{k\text{ten}}$ Potenzen der Wurzeln von f, also

$$\alpha^{p^k}, \beta^{p^k}, \gamma^{p^k}, \ldots$$

sind. Die Coëfficienten von F:

$$A_1 = -\Sigma\alpha^{p^k}, A_2 = \Sigma\alpha^{p^k}\beta^{p^k}, A_3 = -\Sigma\alpha^{p^k}\beta^{p^k}\gamma^{p^k} \ldots$$

sind als ganzzahlige symmetrische Functionen der $\alpha, \beta, \gamma, \ldots$ rational und ganzzahlig durch die $a_1, a_2, \ldots$ darstellbar, und sind daher ganze Zahlen. Die Quotienten

$$\frac{A_1 - a_1^{p^k}}{p}, \quad \frac{A_2 - a_2^{p^k}}{p}, \quad \frac{A_3 - a_3^{p^k}}{p}, \ldots$$

sind aber nach der Formel (1) gleichfalls ganze Zahlen, und es ist also nach dem Fermat'schen Satze

$$(2) \qquad F(x) \equiv f(x) \pmod{p}.$$

Diese Sätze sollen nun auf die Function $f_n(x)$ angewandt werden, deren Wurzeln die sämmtlichen primitiven n^{ten} Einheitswurzeln $\alpha, \beta, \gamma, \ldots$ sind, und die, wie im §. 133 des ersten Bandes bewiesen ist, ganzzahlige Coëfficienten $a_1, a_2, \ldots$ hat.

Ist p eine in n aufgehende Primzahl, so ist

$$(3)\qquad \frac{x^n - 1}{x^{\frac{n}{p}} - 1} = x^{\frac{n}{p}(p-1)} + x^{\frac{n}{p}(p-2)} + \cdots + x^{\frac{n}{p}} + 1,$$

und diese Function verschwindet für $x = \alpha, \beta, \gamma, \ldots$ und ist daher durch $f_n(x)$ theilbar. Wir wollen sie $= f_n(x)\, g(x)$ setzen, worin dann $g(x)$ (nach Bd. I, §. 2) eine ganze Function von x mit ganzzahligen Coëfficienten ist.

Ist nun

$$n = p^k n',$$

n' nicht mehr durch p theilbar, und α' eine primitive n'^{te} Einheitswurzel, so ist

$$\alpha'^{\frac{n}{p}} = 1,$$

und folglich, wenn man $x = \alpha'$ setzt [nach (3)]:

$$(4)\qquad f_n(\alpha')\, g(\alpha') = p.$$

Wir leiten hieraus zunächst einen Beweis für die Irreducibilität von $f_n(x)$ unter der Voraussetzung ab, dass n eine Primzahlpotenz ist, wenn auch für diesen Fall der in Bd. I. §. 134 gegebene Beweis einwandsfrei ist.

Angenommen, es zerfalle $f_n(x)$ in zwei rationale Factoren:

$$(5)\qquad f_n(x) = \varphi(x)\, \psi(x).$$

Dann sind alle Wurzeln, sowohl von $\varphi(x)$ als von $\psi(x)$, n^{te} Einheitswurzeln, und ihre n^{ten} Potenzen also gleich 1. Wenn nun $n = p^k$ ist, so können wir aus $\varphi(x)$ und $\psi(x)$ zwei ganze Functionen $\Phi(x)$, $\Psi(x)$ ableiten, deren Wurzeln die n^{ten} Potenzen der Wurzeln von $\varphi(x)$ und $\psi(x)$ sind und die daher alle gleich 1 sind, und aus (2) ergiebt sich:

$$\varphi(x) \equiv \Phi(x), \quad \psi(x) \equiv \Psi(x) \pmod{p},$$

woraus für $x = 1$ folgt:

$$\varphi(1) \equiv 0, \quad \psi(1) \equiv 0 \pmod{p}.$$

Hiernach ergiebt sich aus (5):

$$(6)\qquad f_n(1) \equiv 0 \pmod{p^2}.$$

Nun ist aber in diesem Falle $f_n(1) = p$ (Bd. I, §. 133, V.), was der Formel (6) widerspricht. Unsere Annahme war also unzulässig und $f_n(x)$ ist irreducibel.

Um die Irreducibilität für ein beliebig zusammengesetztes n nachzuweisen, wenden wir die vollständige Induction an. Wir setzen

$$n = p^k n',$$

und verstehen unter p eine Primzahl, die in n, aber nicht in n' aufgeht, und setzen die Irreducibilität von $f_{n'}(x)$ schon als bewiesen voraus. Ist dann $f_n(x)$ in zwei rationale Factoren $\varphi(x)$, $\psi(x)$ zerlegbar, deren keiner constant ist:

$$(7) \qquad f_n(x) = \varphi(x)\,\psi(x),$$

so leiten wir aus $\varphi(x)$ die Function $\Phi(x)$ ab, deren Wurzeln die $p^{k\text{ten}}$ Potenzen der Wurzeln von $\varphi(x)$ sind, die der Bedingung

$$\varphi(x) \equiv \Phi(x) \pmod{p}$$

genügt, oder auch, indem wir mit $\chi(x)$ eine zweite ganzzahlige Function von x bezeichnen:

$$\varphi(x) = \Phi(x) + p\,\chi(x).$$

Die Wurzeln von $\Phi(x)$ sind aber primitive Einheitswurzeln vom Grade n', und daher muss unter diesen wenigstens eine sein, α', für die $\Phi(\alpha')$ verschwindet, also

$$\varphi(\alpha') = p\,\chi(\alpha')$$

ist. Wegen der vorausgesetzten Irreducibilität von $f_{n'}(x)$ muss aber diese Gleichung für alle Einheitswurzeln α' bestehen, und aus dem gleichen Grunde ist, wenn $\vartheta(x)$ eine ganzzahlige Function ist, für alle α':

$$\psi(\alpha') = p\,\vartheta(\alpha').$$

Hiernach folgt aus (7):

$$f_n(\alpha') = p^2\,\chi(\alpha')\,\vartheta(\alpha'),$$

und nach (4):

$$1 = p\,\chi(\alpha')\,\vartheta(\alpha')\,g(\alpha').$$

Das Product $\chi(x)\,\vartheta(x)\,g(x)$ ist aber eine ganze ganzzahlige Function von x, deren Rest bei der Division mit $f_{n'}(x)$ gleichfalls ganzzahlige Coëfficienten hat und mit $\Theta(x)$ bezeichnet sein mag. Dieser Rest ist von niedrigerem Grade, als $f_{n'}(x)$, und die Function

$$p\,\Theta(x) - 1$$

verschwindet für alle Wurzeln von $f_{n'}(x)$. Folglich muss die Gleichung

$$p\,\Theta(x) = 1$$

identisch sein, was aber offenbar unmöglich ist, da $\Theta(x)$ für ein

ganzzahliges x in eine ganze Zahl übergeht, die, mit p multiplicirt, nicht $= 1$ sein kann.

Hiermit ist die Irreducibilität von $f_n(x)$ allgemein bewiesen.

Nachdem so die Irreducibilität der Kreistheilungsgleichung $f_n(x) = 0$ allgemein nachgewiesen ist, folgt, wie im §. 184 des ersten Bandes, dass sie auch irreducibel bleibt, wenn eine beliebige Einheitswurzel adjungirt wird, deren Grad zu n relativ prim ist.

Kronecker geht gewissermaassen den umgekehrten Weg[1]. Er beweist zunächst unter der Voraussetzung, dass n eine Potenz einer Primzahl p ist, die Irreducibilität von $f_n(x)$ nach Adjunction einer Einheitswurzel, deren Grad nicht durch p theilbar ist, und leitet daraus den allgemeinen Irreducibilitätsbeweis ab, wie wir jetzt noch kurz zeigen wollen.

Es sei jetzt

$$n = p^k$$

eine Potenz einer Primzahl p und

$$(8) \qquad f_n(x) = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \cdots + x^{p^{k-1}} + 1$$

die Function, deren Wurzeln die primitiven n^{ten} Einheitswurzeln sind. Es sei ferner α irgend eine Einheitswurzel, deren Grad m durch p nicht theilbar ist, und ν der Grad des Körpers $R(\alpha)$. Es soll bewiesen werden, dass $f_n(x)$ im Körper $R(\alpha)$ irreducibel ist.

Jede Zahl des Körpers $R(\alpha)$ lässt sich auf eine und nur auf eine Weise in der Form darstellen:

$$(9) \qquad \varphi(\alpha) = m_0 + m_1 \alpha + \cdots + m_{\nu-1} \alpha^{\nu-1},$$

worin $m_0, m_1, \ldots, m_{\nu-1}$ rationale Zahlencoëfficienten sind.

Ist $\chi(x) = 0$ die rationale Gleichung niedrigsten Grades, deren Wurzel α ist, und

$$(10) \qquad \chi(x) = x^\nu + c_1 x^{\nu-1} + \cdots + c_{\nu-1} x + c_\nu,$$

[1] Mém. sur les facteurs irréd. de l'expression $(x^n - 1)$. Liouville's Journal, Bd. 19 (1854). Einen auf der Theorie der höheren Congruenzen beruhenden einfachen Beweis der Irreducibilität der allgemeinen Kreistheilungsgleichung hat Dedekind gegeben [Crelle's Journal für Mathematik, Bd. 58 (1859)].

so sind die $c_1, c_2, \ldots$ ganze Zahlen, weil $\chi(x)$ ein Theiler von $x^m - 1$ sein muss (nach dem Gauss'schen Satze, Bd. I, §. 2).

Daraus ergiebt sich, dass, wenn $\varphi(x)$ eine ganze Function von x mit ganzzahligen rationalen Coëfficienten bedeutet, auch wenn der Grad von $\varphi(x)$ ursprünglich höher als ν ist, die Coëfficienten $m_0, m_1, \ldots, m_{\nu-1}$ in (9) ganze Zahlen werden; denn diese Coëfficienten erhält man, wenn man den Rest der Division von $\varphi(x)$ durch $\chi(x)$ aufsucht.

Wir nehmen nun an, $f_n(x)$ sei im Körper $R(\alpha)$ zerlegbar, und es sei demnach:

(11) $$f_n(x) = \varphi(x, \alpha)\, \psi(x, \alpha),$$

worin $\varphi(x, \alpha)$ und $\psi(x, \alpha)$ zwei ganze Functionen von x sind, deren keine constant ist, deren Coëfficienten in $R(\alpha)$ enthalten sind. Aus (8) und (11) ergiebt sich, wenn wir $x = 1$ setzen,

(12) $$p = \varphi(1, \alpha)\, \psi(1, \alpha),$$

worin $\varphi(1, \alpha)$, $\psi(1, \alpha)$ als Zahlen des Körpers $R(\alpha)$ in der Form (9) darstellbar sind. Bezeichnen wir die kleinsten gemeinschaftlichen Nenner dieser beiden Darstellungen mit a und b, so erhalten wir:

(13) $$\begin{aligned} a\,\varphi(1, \alpha) &= a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_{\nu-1} \alpha^{\nu-1} = A(\alpha) \\ b\,\psi(1, \alpha) &= b_0 + b_1 \alpha + b_2 \alpha^2 + \cdots + b_{\nu-1} \alpha^{\nu-1} = B(\alpha), \end{aligned}$$

worin $a, a_0, a_1, \ldots, a_{\nu-1}$ ganze Zahlen ohne gemeinsamen Theiler und A ein Functionszeichen ist. Gleiches gilt für $b, b_0, b_1, \ldots, b_{\nu-1}$ und B.

Die Wurzeln der Gleichung $\varphi(x, \alpha) = 0$ finden sich unter den primitiven n^{ten} Einheitswurzeln, und diese sind sämmtlich Potenzen von einer unter ihnen, r. Demnach giebt es gewisse Potenzen $r^h, r^{h'}, r^{h''}, \ldots$, so dass

$$\varphi(x, \alpha) = (x - r^h)(x - r^{h'})(x - r^{h''}) \ldots$$

wird, und folglich nach (13):

$$A(\alpha) = a(1 - r^h)(1 - r^{h'})(1 - r^{h''}) \ldots$$

Nehmen wir hiervon die n^{te} Potenz, so ergiebt sich nach (1), mit Rücksicht auf die Gleichung $r^n = 1$:

$$[A(\alpha)]^n = p\, \chi(r),$$

worin $\chi(x)$ eine ganze Function der Variablen x mit ganzzahligen Coëfficienten bedeutet.

Nun setzen wir, indem wir unter t eine Variable verstehen:

$$[t - \chi(1)]\,[t - \chi(r)] \ldots [t - \chi(r^{n-1})] =$$
$$t^n + A_1 t^{n-1} + A_2 t^{n-2} + \cdots + A_n,$$

worin die Coëfficienten $A_1, A_2, \ldots, A_n$ als ganze symmetrische Functionen der n Grössen $\chi(1), \chi(r), \ldots, \chi(r^{n-1})$ ganze rationale Zahlen sind. Wenn wir aber darin

$$t = \chi(r) = \frac{[A(\alpha)]^n}{p}$$

setzen, so verschwindet die linke Seite, und es ergiebt sich durch Multiplication mit p^n:

(14) $$[A(\alpha)]^{n^2} = p\, C(\alpha),$$

wenn $C(\alpha)$ eine Zahl von der Form (9) mit ganzzahligen Coëfficienten bedeutet.

Wenn man die Formel (14) wiederholt in die p^{te} Potenz erhebt und den Satz (1) anwendet, so ergiebt sich daraus für jede Potenz, die nicht kleiner als n^2 ist:

(15) $$A(\alpha^{p^\lambda}) = p\,\xi(\alpha),$$

worin die ganze Function $\xi(\alpha)$ gleichfalls ganzzahlige Coëfficienten hat.

Hierin können wir λ durch $\varphi(m)$ theilbar annehmen, und dann ist, da m durch p nicht theilbar ist, nach dem verallgemeinerten Fermat'schen Satze (Bd. II, §. 14):

$$p^\lambda \equiv 1 \pmod{m}, \quad \alpha^{p^\lambda} = \alpha,$$

so dass aus (14) folgt:

(16) $$A(\alpha) = p\,\xi(\alpha).$$

Es sind daher in (13) die Coëfficienten $a_0, a_1, \ldots, a_{\nu-1}$ alle durch p theilbar und a ist folglich nicht durch p theilbar. Ebenso wird gezeigt, dass $b_0, b_1, \ldots, b_{\nu-1}$ durch p theilbar sind, während b durch p untheilbar ist.

Demnach ergiebt sich aus (12), wenn $A(\alpha)\,B(\alpha) = p^2\,\Theta(\alpha)$ gesetzt wird:

(17) $$a b = p\,\Theta(\alpha),$$

worin $\Theta(\alpha)$ eine Function von α von der Form (9) mit ganzzahligen Coëfficienten bedeutet. Die Gleichung (17) müsste aber, da sie höchstens vom $(\nu-1)^{\text{ten}}$ Grade ist, in Bezug auf α identisch sein, und es müsste ab durch p theilbar sein, was nicht möglich ist.

Hieraus folgt die Unzulässigkeit unserer Annahme, dass $f_n(x)$ nach der Formel (11) im Körper $R(\alpha)$ in zwei Factoren zerlegbar ist.

Damit lässt sich nun aufs Neue allgemein beweisen, dass die Gleichung, deren Wurzeln die sämmtlichen primitiven m^{ten} Einheitswurzeln sind, deren Grad $\varphi(m)$ ist, auch wenn m eine beliebige zusammengesetzte Zahl ist, irreducibel ist. Dies ist mit folgendem Satze gleichbedeutend:

> Wenn eine ganze Function $\varphi(x)$ mit rationalen Coëfficienten verschwindet, wenn für x eine primitive m^{te} Einheitswurzel gesetzt wird, so verschwindet $\varphi(x)$ auch, wenn für x irgend eine andere primitive m^{te} Einheitswurzel gesetzt wird.

Wenn m eine Primzahlpotenz ist, so ist der Satz in dem Vorhergehenden schon bewiesen. Wir wenden daher die vollständige Induction an, nehmen ihn für m^{te} Einheitswurzeln als erwiesen an und leiten ihn für mn^{te} Einheitswurzeln her, wenn $n = p^k$ und p eine in m nicht aufgehende Primzahl ist.

Jede mn^{te} Einheitswurzel β kann in der Form

$$\beta = \alpha r$$

dargestellt werden, worin α eine m^{te}, r eine n^{te} Einheitswurzel ist. Was zu beweisen ist, lässt sich so aussprechen, dass, wenn β die Wurzel einer rationalen Gleichung $\Phi(x) = 1$ ist, auch alle anderen primitiven Einheitswurzeln vom Grade mn Wurzeln dieser Gleichung sein müssen.

Ist, wie oben, $f_n(x) = 0$ die Gleichung, deren Wurzeln die Grössen r sind, so ist, wie wir bewiesen haben, $f_n(x)$ nicht in rationale Factoren zerlegbar, auch nicht in solche, die rational von α abhängen. Die Function $f_n(\alpha^{-1}x)$, die für $x = \beta$ verschwindet, kann also auch nicht in rationale Factoren zerlegt werden, weil aus einer Zerlegung der Form

$$f_n(\alpha^{-1}x) = \varphi(x, \alpha)\, \psi(x, \alpha)$$

folgen würde:

$$f_n(x) = \varphi(\alpha x, \alpha)\, \psi(\alpha x, \alpha),$$

was nicht bestehen kann. Da hiernach $f_n(\alpha^{-1}x)$ eine Wurzel

mit $\Phi(x)$ gemein hat, so muss $\Phi(x)$ durch $f_n(\alpha^{-1}x)$ theilbar sein, und wir können demnach für ein unbestimmtes x

(18) $$\Phi(x) = f_n(\alpha^{-1}x)\, \Psi(x, \alpha)$$

setzen, worin $\Psi(x, \alpha)$ eine ganze rationale Function von x ist.

Sind $\alpha, \alpha_1, \alpha_2, \ldots$ die sämmtlichen primitiven m^{ten} Einheitswurzeln, die, wie wir angenommen haben, Wurzeln einer irreduciblen rationalen Gleichung

$$F_m(x) = 0$$

sind, so kann α nach dieser Voraussetzung in der Identität (18) durch jedes andere $\alpha_1, \alpha_2, \ldots$ ersetzt werden, und es folgt, dass $\Phi(x)$ durch jeden der Factoren

$$f_n(\alpha^{-1}x),\ f_n(\alpha_1^{-1}x),\ f_n(\alpha_2^{-1}x) \ldots$$

theilbar ist. Zwei dieser Factoren können aber keinen gemeinschaftlichen Theiler haben, denn wenn etwa

$$f_n(\alpha^{-1}x) = 0,\ f_n(\alpha_1^{-1}x) = 0$$

eine gemeinsame Wurzel x hätten, so müssten zwei primitive n^{te} Einheitswurzeln r, r_1 existiren, so dass

$$x = \alpha r = \alpha_1 r_1$$

wäre; es müsste also $\alpha^n = \alpha_1^n$, und folglich, da n relativ prim zu m ist, $\alpha = \alpha_1$ sein.

Demnach ist $\Phi(x)$ theilbar durch das Product

$$F_{mn}(x) = f_n(\alpha^{-1}x)\, f_n(\alpha_1^{-1}x)\, f_n(\alpha_2^{-1}x) \ldots,$$

dessen Wurzeln die sämmtlichen β sind, und diese Function ist daher auch unzerlegbar, wie bewiesen werden sollte.

II.

Die Irreducibilität der Kreistheilungsgleichung und der Satz über die in einer Linearform enthaltenen Primzahlen.

Während im ersten Nachtrage, der als Ergänzung zum ersten Bande zu betrachten ist, absichtlich kein Gebrauch von der Theorie der ganzen algebraischen Zahlen gemacht ist, geben wir zum Schluss noch einen auf anderen Grundlagen, nämlich auf den Sätzen über die Classenzahl (§. 192) beruhenden Beweis für die Irreducibilität der Kreistheilungsgleichung, der wegen der Verallgemeinerungen, die er zulässt, merkwürdig ist.

Es sei m eine beliebige natürliche Zahl, und n sei das System der zu m theilerfremden positiven Zahlen; unter diesen giebt es

(1) $$\varphi(m) = \mu,$$

die kleiner als m sind, die wir mit a bezeichnen.

Wenn wir alle nach dem Modul m mit einem a congruenten Zahlen n in eine Classe A vereinigen, so erhalten wir μ Zahlclassen:

(2) $$A_1, A_2, \ldots, A_\mu,$$

die bei der Composition durch Multiplication eine Abel'sche Gruppe μ^{ten} Grades, $\mathfrak{N}$, bilden. Diese Gruppe ist schon im §. 16 dieses Bandes betrachtet.

Die μ Charaktere dieser Gruppe bezeichnen wir mit

(3) $$\chi_1, \chi_2, \ldots, \chi_\mu,$$

und setzen, wenn χ einer dieser Charaktere ist, und n eine Zahl aus der Classe A bedeutet,

(4) $$\chi(A) = \chi(n).$$

Diese Charaktere, die im §. 16 näher bestimmt sind, sind sämmtlich μ^{te} Einheitswurzeln.

Wir haben aber hier nicht nöthig, von den speciellen Ausdrücken dieser Charaktere Gebrauch zu machen. Dahingegen stützen wir uns auf folgenden Lehrsatz, der für alle Abel'schen Gruppen gilt:

1. Ist A ein Element f^{ten} Grades einer Abel'schen Gruppe μ^{ten} Grades, und ist $\mu = ef$, so sind alle $\chi_i(A)$ f^{te} Einheitswurzeln, und darunter kommt jede f^{te} Einheitswurzel genau e mal vor.

Der Satz ist implicite in dem Satze 7., §. 12 dieses Bandes enthalten. Denn wenden wir diesen Satz auf die Gruppe

$$T = 1, A, A^2, \ldots, A^{f-1}$$

an, deren Index in Bezug auf $\mathfrak{N}$ gleich e ist, so folgt, dass es eine Gruppe Ξ von e Charakteren ξ giebt, die den Bedingungen

$$\xi(A) = 1$$

genügen.

Zerlegt man also die Gruppe X der Charaktere χ in die Nebengruppen

$$\Xi_1, \Xi_2, \ldots, \Xi_f,$$

so sind $\chi_1(A)$ und $\chi_2(A)$ einander gleich oder von einander verschieden, je nachdem χ_1 und χ_2 in derselben oder in verschiedenen dieser Nebengruppen vorkommen. Da ausserdem wegen $\chi(A)^f = \chi(A^f) = 1$ alle $\chi(A)$ Einheitswurzeln vom Grade f sind, und es nur f verschiedene solche giebt, so ist damit unser Theorem bewiesen.

Ist n in der Classe A enthalten, so ist der Grad f von A der Exponent, zu dem n nach dem Modul m gehört, d. h. der kleinste positive Exponent, für den

$$n^f \equiv 1 \pmod{m} \tag{5}$$

ist. Wenn also n zum Exponenten f gehört, so sind alle $\chi_i(n)$ f^{te} Einheitswurzeln, und jede f^{te} Einheitswurzel kommt darunter e mal vor.

Bedeutet a irgend einen der $\varphi(m)$ Reste der Zahlen n, so ist in der Form

$$\mu_x = mx + a - m \tag{6}$$

jede Zahl aus der durch a repräsentirten Zahlclasse (2) enthalten; verstehen wir unter a den kleinsten positiven Rest, so erhalten wir die Gesammtheit der Zahlen dieser Classe, wenn wir x alle positiven ganzzahligen Werthe durchlaufen lassen.

Nun ist

$$\frac{\mu_x}{m} - x = \frac{a - m}{m},$$

und folglich können wir auf die Grössen μ_x den Satz §. 191, 6. anwenden, in dem wir $n = x$, $\gamma = 1 : m$, $c_n = (a - m) : m$ zu setzen haben. Es ist also

$$(7) \qquad A(s) = \sum_{0,\infty}^{x} \frac{1}{(mx + a)^s} = \sum_{1,\infty}^{x} \frac{1}{(mx + a - m)^s},$$

so lange $s > 1$ ist, eine stetige Function von s, und es ist

$$(8) \qquad A(s) = \frac{1}{m(s-1)} + C(s),$$

worin $C(s)$ für $s = 1$ endlich bleibt[1]).

Wir lassen nun A die sämmtlichen Classen (2) durchlaufen, bezeichnen mit χ irgend einen der Charaktere der Gruppe $\mathfrak{R}$ und setzen

$$(9) \qquad Q(s) = \sum^{A} \chi(A)\, A(s),$$

oder, was dasselbe ist,

$$(10) \qquad Q(s) = \sum^{n} \frac{\chi(n)}{n^s},$$

worin sich die Summe auf alle Zahlen n erstreckt. Die Anzahl dieser Summen Q ist so gross, als die Anzahl der Charaktere, d. h. $= \varphi(m)$. Wir bezeichnen sie, wenn eine Unterscheidung nöthig ist, mit

$$Q_1, Q_2, \ldots, Q_\mu.$$

Eine von ihnen, Q_1, entspricht dem Hauptcharakter und hat den Ausdruck

$$Q_1(s) = \sum^{n} \frac{1}{n^s}.$$

Nun ist [§. 11, (21)]:

$$\sum^{A} \chi(A) = \mu \text{ oder } = 0,$$

je nachdem χ der Hauptcharakter ist oder nicht. Ferner ergiebt sich aus (8)

---

1) Durch Benutzung bekannter Sätze über Γ-Functionen findet man nach §. 191, (20):

$$C(1) = \frac{1}{m} \frac{\Gamma'\left(\frac{a}{m}\right)}{\Gamma\left(\frac{a}{m}\right)}.$$

$$Q(s) = \frac{1}{m(s-1)} \overset{A}{\Sigma}\, \chi(A) + \overset{A}{\Sigma}\, \chi(A)\, C(s),$$

und daraus der Satz:

2. Die Summen $Q_2, \ldots, Q_\mu$ erhalten für $s = 1$ endliche Werthe, Q_1 wird unendlich, und zwar wird

$$\operatorname*{Lim}_{s=1} (s-1)\, Q_1(s) = \frac{\mu}{m}.$$

Um die Summen $Q(s)$ umzuformen, bezeichnen wir mit p jede in m nicht aufgehende Primzahl und multipliciren alle die unendlichen Reihen von der Form

$$1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots = \frac{1}{1 - \chi(p)\, p^{-s}}$$

mit einander. Dadurch erhalten wir [vgl. §. 192, (8)]:

(11) $$Q(s) = \overset{p}{\Pi}\, \frac{1}{1 - \chi(p)\, p^{-s}}.$$

Wenn nun p zum Exponenten f gehört, wenn also f die kleinste positive, der Congruenz

(12) $$p^f \equiv 1 \pmod{m}$$

genügende Zahl, und $\mu = ef$ ist, so kommt unter den $\chi(p)$ jede f^{te} Einheitswurzel genau e mal vor, und es ist also (für ein variables x):

$$\overset{\chi}{\Pi}\, [1 - \chi(p)\, x] = (1 - x^f)^e,$$

demnach ergiebt sich aus (11):

(13) $$Q_1\, Q_2 \ldots Q_\mu = \overset{p}{\Pi}\, \frac{1}{(1 - p^{-fs})^e}.$$

Wir führen nun, ohne die Irreducibilität der Kreistheilungsgleichung vorauszusetzen, den Kreistheilungskörper Ω_m ein, dessen noch unbekannten Grad wir mit ν bezeichnen wollen. Da aber die primitive m^{te} Einheitswurzel r einer rationalen Gleichung μ^{ten} Grades genügt, so ist

(14) $$\nu \leqq \mu.$$

Die Zahlen ω des Körpers Ω_m sind alle in der Form

(15) $$a\,\omega = a_0 + a_1 r + \cdots + a_{\nu-1} r^{\nu-1}$$

mit ganzen rationalen Coëfficienten $a, a_0, a_1, \ldots, a_{\nu-1}$ darstellbar, und wenn ω eine ganze Zahl ist, so können wir für a eine feste ganze Zahl setzen, deren nähere Kenntniss nicht erforder-

lich ist. Ihr Werth ist gleich der Quadratwurzel aus dem Quotienten der Discriminanten

$$\Delta\,(1, r, r^2, \ldots, r^{\nu-1}) : \Delta\,(\omega_1, \omega_2, \ldots, \omega_\nu),$$

worin $\omega_1, \omega_2, \ldots, \omega_\nu$ eine Minimalbasis ist (§. 144, 145).

Wir schliessen alle in der Discriminante der Kreistheilungsgleichung und alle in m und in a aufgehenden Primzahlen, deren Anzahl jedenfalls endlich ist, von dem Systeme der p aus, und bezeichnen mit $\mathfrak{p}$ ein in p aufgehendes Primideal. Dann ist die Congruenz

$$r^p \equiv r \pmod{\mathfrak{p}}$$

immer dann, aber auch nur dann, erfüllt, wenn

$$(16) \qquad p \equiv 1 \pmod{m}$$

ist, d. h. wenn p zum Exponenten 1 gehört, wenn also $r^p = r$ ist, und unter derselben Bedingung ist daher auch nach (15) für jede ganze Zahl ω in Ω_m:

$$\omega^p \equiv \omega \pmod{\mathfrak{p}}.$$

Dies ist aber nach §. 162 die nothwendige und hinreichende Bedingung dafür, dass die in der Körperdiscriminante von Ω_m nicht aufgehende Primzahl p in lauter Primideale ersten Grades zerfällt.

Bezeichnen wir also mit

$$P_f(s) = \Pi\,(1 - p^{-sf})$$

das über alle zum Exponenten f gehörigen Primzahlen p erstreckte Product, so ergiebt sich aus §. 192, dass, wenn $f > 1$ ist, $P_f(1)$ endlich und von Null verschieden ist, und dass

$$(17) \qquad \frac{s-1}{P_1(s)^\nu}$$

für $s = 1$ endlich und von Null verschieden ist.

Nun ist nach (13), wenn mit S das über die ausgeschlossenen Primzahlen p erstreckte endliche Product $\Pi\,(1 - p^{-sf})^{-e}$ bezeichnet wird,

$$Q_1\, Q_2 \ldots Q_\mu = S \prod^f \frac{1}{P_f(s)^e},$$

und da $e = \mu$ für $f = 1$, so ergiebt sich aus (17):

$$(18) \qquad (s-1)^{\frac{\mu}{\nu}}\, Q_1\, Q_2 \ldots Q_\mu$$

für $s = 1$ endlich und von Null verschieden.

Andererseits ist aber nach 2.:

(19) $$(s-1)\, Q_1 Q_2 \ldots Q_\mu$$

für $s = 1$ endlich, und wenn wir also (19) durch (18) dividiren, so folgt:

$$(s-1)^{1-\frac{\mu}{\nu}} \text{ für } s = 1 \text{ endlich,}$$

d. h.

(20) $$\nu \gtreqless \mu.$$

Dies mit (14) zusammen ergiebt aber $\nu = \mu$, wodurch der folgende Satz bewiesen ist:

3. Der Grad des Kreistheilungskörpers Ω_m ist gleich $\varphi(m)$, also die Kreistheilungsgleichung $\varphi(m)^{\text{ten}}$ Grades, deren Wurzeln die primitiven m^{ten} Einheitswurzeln sind, irreducibel.

Diese Betrachtung leistet uns aber noch einen anderen wichtigen Dienst, indem sie uns den Beweis des berühmten Satzes liefert, dass in jeder arithmetischen Progression, deren Differenz und Anfangsglied natürliche Zahlen ohne gemeinsamen Theiler sind, unendlich viele Primzahlen enthalten sind[1]).

Es folgt nämlich jetzt aus (18), dass das Product

$$(s-1)\, Q_1 Q_2 \ldots Q_\mu$$

für $s = 1$ einen endlichen und von Null verschiedenen Werth hat, und da nach 2. keiner der Factoren unendlich ist, so folgt:

4. Die Summen

$$(s-1)\, Q_1(s),\ Q_2(s), \ldots, Q_\mu(s)$$

haben für $s = 1$ endliche und von Null verschiedene Werthe.

Wenden wir auf alle Factoren von (11) die Formel an:

$$\log\left[1 - \chi(p)\, p^{-s}\right] = \frac{\chi(p)}{p^s} + \frac{1}{2}\frac{\chi(p^2)}{p^{2s}} + \frac{1}{3}\frac{\chi(p^3)}{p^{3s}} + \cdots$$

---

[1]) Der erste vollständige und allgemeine Beweis dieses Satzes ist von Dirichlet gegeben (Abhandlungen der Berl. Akademie vom Jahre 1837. Gesammelte Werke Nr. XXI). Auf die wesentliche Vereinfachung dieses Beweises durch Benutzung der Kummer'schen Formeln für die Classenzahl in den Kreistheilungskörpern hat Dedekind aufmerksam gemacht (Vorlesungen über Zahlentheorie, 3. Auflage, S. 596).

(worin der imaginäre Theil des Logarithmus zwischen $\pm \pi i$ zu nehmen ist), so folgt, wenn der imaginäre Theil von $\log Q(s)$ passend bestimmt wird,

$$(21) \qquad \log Q(s) = \Sigma \frac{\chi(p)}{p^s} + \tfrac{1}{2} \Sigma \frac{\chi(p^2)}{p^{2s}} + \tfrac{1}{3} \Sigma \frac{\chi(p^3)}{p^{3s}} + \cdots$$

Wenn nun A irgend eine der Classen (2) und a eine Zahl aus A bedeutet, so ist nach §. 11, (6) dieses Bandes

$$(22) \qquad \overset{\chi}{\Sigma}\, \chi(A)\, \chi(n) = \Sigma\, \chi(an) = \mu \text{ oder } = 0,$$

je nachdem $an \equiv 1$ oder nicht $\equiv 1$ nach dem Modul m ist, d. h. je nachdem n in der Classe A^{-1} enthalten ist oder nicht enthalten ist. Wenn wir also die Formel (21) mit $\chi(A)$ multipliciren und in Bezug auf χ summiren, so folgt

$$(23) \qquad \frac{1}{\mu} \overset{\chi}{\Sigma}\, \chi(A) \log Q(s) =$$
$$\Sigma \frac{1}{p^s} + \tfrac{1}{2} \Sigma \frac{1}{p^{2s}} + \tfrac{1}{3} \Sigma \frac{1}{p^{3s}} + \cdots,$$

wo sich rechts die erste, zweite, dritte, ... Summe auf alle Primzahlen p bezieht, deren erste, zweite, dritte, ... Potenz in A^{-1} enthalten ist.

Der zweite Theil dieser Summe

$$R(s) = \tfrac{1}{2} \Sigma \frac{1}{p^{2s}} + \tfrac{1}{3} \Sigma \frac{1}{p^{3s}} + \cdots$$

wird vergrössert, wenn man jede seiner Theilsummen auf alle Primzahlen p erstreckt, und demnach ist

$$R(s) < \tfrac{1}{2} \Sigma \left(\frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) = \tfrac{1}{2} \Sigma \frac{1}{p^s(p^s - 1)},$$

also um so mehr:

$$R(s) < \tfrac{1}{2} \sum_{2,\infty}^{n} \frac{1}{n^{2s}(1 - n^{-s})},$$

oder, da $1 - n^{-s} > \frac{1}{2}$ ist:

$$R(s) < \sum_{2,\infty}^{n} \frac{1}{n^{2s}},$$

und hieraus schliesst man, dass R für $s = 1$ endlich bleibt (§. 191, 2.).

Wenn wir nun in der Formel (23),

$$\frac{1}{\mu} \overset{\chi}{\Sigma}\, \chi(A) \log Q(s) = \Sigma \frac{1}{p^s} + R(s),$$

s in 1 übergehen lassen, so wird $\log Q_1(s)$ nach 4. unendlich, während die übrigen Glieder der linken Seite, $\log Q_2(s), \ldots \log Q_\mu(s)$, endlich bleiben. Da $R(s)$ gleichfalls endlich bleibt, so muss die Summe $\sum p^{-s}$ unendlich werden, und dies ist sicher nur dann möglich, wenn die Summe aus unendlich vielen Gliedern besteht. Hiermit ist bewiesen:

5. In jeder der Zahlclassen A (nach dem Modul m) sind unendlich viele Primzahlen enthalten.

Man kann dies auch so ausdrücken, dass die Linearform $mx + a$, in der m und a ganze Zahlen ohne gemeinsamen Theiler sind, für unendlich viele ganzzahlige Werthe von x eine Primzahl darstellt.

REGISTER.

(Die römischen Ziffern bezeichnen den Band, die arabischen Ziffern die Seite.)

Berichtigungen zum ersten Bande.

Seite 93, Zeile 6 v. u. lies $B_h^{(i)}$ statt $B^{(i)}$.

„ 117, Formel (10) lies $\sqrt[3]{\frac{-b}{2} + \sqrt{R}}$ statt $\sqrt{\frac{-b}{2} + \sqrt{R}}$.

„ 158, Formeln (14) rechts m und n zu vertauschen.

„ 172, Formel (14) lies $n - 1$ statt $n + 1$.

„ 185, Zeile 9 v. o. „ Φ' statt Φ.

„ 190, „ 11 v. u. „ a_1' „ $(n - 1)\, a_1'$.

„ 194, „ 7 v. u. „ $+9$ „ -9.

„ 200, „ 7 v. u. „ §. 61 „ §. 67.

„ 202, „ 3 v. u. „ u „ v_1 (in beiden Formeln).

„ 213, „ 6 v. u. „ $\Phi(\tau, \xi)$ statt $\Phi(\tau, k)$.

„ 221, „ 12 v. u. „ $\frac{2}{9}$ statt $\frac{2}{3}$.

„ 222, „ 4, 5 v. u. „ $+q_0, -q_0$ statt $-q_0, +q_0$.

„ 233, „ 4, 7 v. o. „ $\frac{1}{5}D$ statt $5D$.

„ 236, „ 12 v. o. „ $5c^2$ „ $-5c^2$.

„ 251, „ 10 v. o. „ $-\psi'_3$ „ ψ'_3.

„ 268, „ 5 v. u. „ $\frac{1}{5}D$ „ D.

„ 282, Formel (2) „ f_s „ f^s.

„ 318, Zeile 2 v. u. „ $F'(z)$ „ $F'(x)$.

„ 332, Formel (5) „ $f(\beta) -$ statt $f(\beta) +$.

„ 334, Zeile 6 v. u. „ 0,00164 „ 0,0164.

„ 344, „ 6 v. u., Formel, lies $\alpha_n \varphi(\alpha_n)$ und $\varphi(\alpha_n)$ statt $\alpha_m \varphi(\alpha_m)$ in $\varphi(\alpha_m)$.

„ 357, „ 3 v. u. lies 6 statt 5.

„ 378, 379, Formel (13), (14) ist a_1, b_1, c_1 durch $\pm a_1, \pm b_1, \pm c_1$ zu ersetzen, und das Zeichen so zu bestimmen, dass c_1 positiv wird.

„ 402, Zeile 6, 7 v. u. ist $a_4 = 1$ und $a_3 = 2$ zu vertauschen.

„ — „ 4 v. u. lies 9083 statt 9183.

„ 419, Hierzu vergleiche man den I. Nachtrag zum zweiten Bande.

„ 423, Zeile 15 v. o. lies $\frac{(n-1)(n-2)}{2}$ statt $\frac{n \,.\, n-1}{2}$.

„ — „ 24 v. o. ist zu lesen $\frac{1}{2}\left(\frac{(n-1)(n-2)}{2} - \frac{n-1}{2}\right)$

$$= \frac{(n-1)(n-3)}{4} \equiv 0 \pmod 2.$$

Seite 423, Zeile 3 v. u. lies $(-1)^{\frac{(n-1)(n-3)}{4}} = +1$ statt $(-1)^{\frac{n-1}{2}}$.

„ 424, Formel (14) „ $P = i^{\frac{n-1}{2}} n^{\frac{n-3}{2}} \sqrt{n}$.

„ 436, Zeile 3, 22 v. o. lies $\frac{\pi}{n}$ statt π.

„ 482, „ 8 v. u. ist transitiv und intransitiv zu vertauschen.

„ 502, „ 18 v. o. lies π_1 statt π.

„ 504, „ 9 v. u. „ $k_{\varrho-1}$ statt $k_{\nu-1}$.

„ 514, „ 5 v. u. „ Θ_1 statt Θ_i.

„ 531, „ 11 v. o. „ y_1^2 „ y^2.

„ 540, Formel (10) „ γ_{e-1} statt γ_{c-1}.

„ 544, Zeile 15 v. o. „ $m B_k = \sum^{s} \varepsilon^{-k} (\varepsilon, \alpha)^{\nu} (\varepsilon^{\lambda_1}, \alpha)^{\nu_1} (\varepsilon^{\lambda_2}, \alpha)^{\nu_2} \dots$

„ — „ 23 v. o. „ ε^{λ_2} statt ε^2.

„ 551, „ 15 v. o. „ α_k „ α^k.

„ 592, „ 8 v. u. „ die nur erfüllt ist für $b = 0$, $a = \pm 1$ oder $a = 0$, $b = \pm 1$ oder $a = b = \pm 1$.

„ 612, „ 12 v. o. „ $1 - a$ statt $a - b$.

„ 618, „ 1 v. u. „ c_1^h statt c_1.

„ 623, „ 6 v. u. „ α_6 „ α_6.

„ 636, „ 18, 21 v. o. lies $-g^{n-1} + 1$ statt $g^{n-1} - 1$.

„ 639, „ 10, 27 v. o. „ $n-2$, $n-3$ statt $n-1$, $n-2$.

„ 641, „ 1 v. o. lies (6) statt (5).

„ 646, „ 11 v. o. „ rational in $\mathfrak{K}(\mathfrak{t}_0)$ statt rational.

„ — „ 14, 19, 22, 26 v. o. lies $\mathfrak{K}(\mathfrak{t}_0)$ statt $\mathfrak{K}$.

„ — „ 17, 18 v. o. von „Alle Grössen“ an zu streichen.

„ — „ 1, 2 v. u. „ „die anderen“ an zu streichen.

„ 653, „ 4 v. o. lies $-A_4 r \varrho$ statt $+A_4 r \varrho$.

„ — „ 5 v. o. „ $+A_2 \varrho'$ „ $-A_2 \varrho'$.

Berichtigungen zum zweiten Bande.

Seite 15, Zeile 19 v. o. lies N statt P.

„ 16, „ 12, 13 v. o. sind P und Q zu vertauschen.

„ 21, „ 19 v. o. lies (17) statt (13).

„ 26, „ 17 v. o. „ §. 6, 4 statt §. 6, 2.

„ 569, „ 5 v. u. im Exponenten lies $n - \nu$ statt $\mu - \nu$.

„ 592, „ 6, 3 v. u. lies $\gamma^{P^f - 1}$ statt $\gamma^{P^f} - 1$.